



CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

JULI 2022

CHINA *local global*

Lokalisasi dan Keberhasilan Teknologi China di Indonesia

Gatra Priyandita, Dirk van der Kley, dan Benjamin Herscovitch

Lokalisasi dan Keberhasilan Teknologi China di Indonesia

Gatra Priyandita, Dirk van der Kley,
dan Benjamin Herscovitch

© 2022 Carnegie Endowment for International Peace. All rights reserved.

Carnegie tidak mengambil posisi kelembagaan atas isu-isu kebijakan publik; pandangan-pandangan yang direpresentasikan di sini adalah pendapat penulis (-penulis) dan tidak mencerminkan pendapat Carnegie, staf, atau wali amanat. Dilarang mereproduksi atau mengubah dalam bentuk apapun atau dengan cara apapun publikasi ini atau bagian-bagiannya tanpa ijin tertulis dari the Carnegie Endowment for International Peace. Silakan kirim pertanyaan langsung kepada:

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

Publikasi ini dapat diunduh tanpa biaya pada CarnegieEndowment.org

DAFTAR ISI

China Local/Global	vii
Ringkasan	1
Pendahuluan	3
Tuntutan Pembangunan Indonesia	5
Peran Huawei dan ZTE dalam Insfrastruktur Digital Indonesia	10
Pelatihan dan Pengembangan Kapasitas	16
Visi Lain Keamanan	20
Pelajaran Terpetik	26
Tentang Penulis	28
Catatan	29

China Local/Global

China telah menjadi kekuatan global, namun tampaknya terlalu sedikit perbincangan yang telah dilakukan tentang *bagaimana* fenomena ini terjadi dan apa artinya. Banyak yang berpendapat bahwa China mengeksport model pembangunan dan mengaplikasikannya ke negara-negara lain. Tetapi lembaga pemerintah dan aktor swasta dari China juga memperluas pengaruh mereka dengan cara bekerjasama dengan aktor-aktor dan lembaga-lembaga setempat seraya mengadaptasi dan mengasimilasi model-model serta praktik-praktik lokal dan tradisional.

Dengan hibah dermawan berjangka tahunan dari Ford Foundation, Carnegie telah meluncurkan sebuah badan riset inovatif mengenai strategi keterlibatan China di tujuh kawasan dunia – Afrika, Asia Tengah, Amerika Latin, Timur Tengah dan Afrika Utara, Pasifik, Asia Selatan, dan Asia Tenggara. Melalui serangkaian riset dan pertemuan strategis, proyek ini mengeksplorasi berbagai dinamika kompleks tersebut, termasuk bagaimana perusahaan-perusahaan China beradaptasi dengan undang-undang ketenagakerjaan setempat di Amerika Latin, bank-bank dan badan-badan keuangan China mengeksplorasi produk-produk keuangan dan kredit Islam tradisional di Asia Selatan dan Timur Tengah, dan perusahaan-perusahaan China membantu pekerja-pekerja lokal meningkatkan keahlian mereka di Asia Tengah. Strategi-strategi adaptif China yang mengakomodasi dan berjalan seiring realita lokal adalah yang paling sering diabaikan oleh para pembuat kebijakan di negara Barat.

Pada puncaknya, proyek ini bertujuan untuk secara signifikan memperluas pemahaman dan perbincangan tentang peran China di dunia dan untuk menghasilkan gagasan-gagasan kebijakan inovatif. Ini dapat memungkinkan pemain-pemain lokal untuk dapat lebih menyalurkan energi-energi China dalam mendukung masyarakat dan ekonomi mereka; memberikan pelajaran bagi keterlibatan Barat di seluruh dunia, khususnya di negara-negara berkembang; membantu komunitas kebijakan China sendiri untuk belajar dari keberagaman pengalaman China; dan secara potensial untuk mengurangi gesekan.

Evan A. Feigenbaum

Wakil Presiden bidang Kajian, Carnegie Endowment for International Peace

Ringkasan

Rata-rata, warga Indonesia tidak mempercayai pemerintah dan banyak perusahaan asal China. Namun Huawei, dan pada skala yang lebih kecil ZTE, telah berhasil memposisikan diri mereka sebagai penyedia keamanan siber terpercaya bagi pemerintah, serta juga banyak perusahaan, Indonesia. Ini tentunya bukan prestasi yang mudah diraih mengingat lamanya rasa permusuhan Indonesia terhadap China. Banyak perusahaan China telah menghadapi protes sehubungan dengan kekhawatiran kalau mereka telah mengambil alih pekerjaan lokal. Namun Huawei dan ZTE tak mengalami nasib tersebut. Juga tak ada koalisi besar-besaran dari perwakilan-perwakilan Indonesia yang menentang teknologi China dalam infrastruktur genting telekomunikasi. Pada singkatnya, warga Indonesia lebih peduli pada perusahaan semen China daripada terhadap keterlibatan Huawei di jaringan 5G.

Tentunya ini adalah bahasan yang sangat berbeda dengan yang terjadi di negara-negara demokrasi liberal yang kaya. Huawei dan ZTE sudah mampu meraih kesuksesan di Indonesia, meskipun ada rasa ketidakpercayaan di antara lembaga-lembaga pemerintahan dan pertahanan Indonesia tentang niat China, serta juga meningkatnya sorotan Barat atas penggunaan teknologi China dalam jaringan broadband.

Seperti yang telah ditunjukkan oleh makalah-makalah lain dalam seri ini, Huawei dan ZTE perlu untuk melokalisasi strategi-strategi mereka. Seperti yang terjadi di tempat lain di seluruh dunia, bukti yang ada menunjukkan bahwa bagian nilai manfaat produk Huawei adalah harga yang lebih murah (dibanding harga pesaing-pesaing mereka) untuk teknologi berkualitas tinggi.

Tetapi itu hanyalah sebagian dari kisahnya. Huawei telah memposisikan diri sebagai pilihan penyedia keamanan siber untuk banyak organisasi di Indonesia dengan menawarkan banyak program pelatihan untuk keamanan siber, serta program pelatihan lain, untuk berbagai kelompok mulai dari pejabat-pejabat pemerintahan sampai pada mahasiswa dari pedesaan Indonesia. Banyak dari pelatihan ini secara teknis berfokus pada keahlian kejuruan praktis dengan harapan bahwa mereka itu pada suatu hari akan menjadi konsumen. Sebagai tambahan, perusahaan memberikan paket pemeliharaan dan perawatan yang menarik.

Sejak pertengahan 2000an, perusahaan-perusahaan teknologi informasi dan komunikasi China telah menciptakan pusat-pusat pelatihan dalam kerjasama dengan perusahaan-perusahaan telekomunikasi lokal serta universitas-universitas di Indonesia. Badan-badan pemerintahan juga semakin menargetkan pelatihan dan program pengembangan kapasitas, dengan Huawei mengklaim bahwa 7.000 pejabat pemerintah telah berpartisipasi dalam program pelatihan tersebut. Pemerintah, perusahaan-perusahaan besar Indonesia, dan warga Indonesia kebanyakan juga menyambut Huawei dan ZTE

sebagai mitra penting dalam upaya mereka membangun baik infrastruktur maupun modal manusia yang penting untuk berjaya dalam ekonomi digital di abad 21.

Apa yang ditawarkan oleh Huawei dan ZTE adalah transfer pengetahuan, bukan transfer teknologi. Teknologinya sedang dibangun di China oleh perusahaan-perusahaan China. Namun peran Huawei dalam pelatihan berkenaan dengan pengembangan kapasitas, warga Indonesia akan memasang, memelihara, dan menggunakan jaringan, dan China membangun hardware-nya.

Juga ada bukti bahwa China punya keberhasilan retorik dalam mendesak tata kelola versi ruang sibernya sendiri. Bahasa tata kelola ruang siber yang lebih disukai pemerintah China itu dicantumkan dalam Memorandum of Understanding (MoU) antara Badan Siber dan Sandi Negara Indonesia (BSSN) dan Badan Administrasi Keamanan Siber China (Cybersecurity Administration of China). Namun begitu, sulit dilihat bagaimana kesepakatan tersebut bisa mempengaruhi praktik tata kelola keamanan siber Indonesia.

Salah satu keprihatinan yang sering disamai oleh negara-negara demokrasi liberal yang kaya adalah bahwa ketergantungan pada teknologi China akan berakhir dengan disejajarkannya kepentingan-kepentingan politis negara-negara seperti Indonesia dengan kepentingan China. Kekhawatiran utama lainnya adalah bahwa kegiatan spionase China tak terhindarkan serta risiko yang terus berjalan (namun belumlah disadari) bahwa perusahaan-perusahaan China dengan peran dominan dalam ekosistem Teknologi Informasi dan Komunikasi (TIK) dapat digunakan oleh pemerintah China untuk menerapkan tekanan politis penuh paksaan.

Meskipun dengan dirangkulnya Huawei dan ZTE oleh Indonesia, pemimpin-pemimpin politik di Jakarta tak begitu saja mengabaikan pertanyaan-pertanyaan berat keamanan yang timbul dengan meng-upgrade peralatan TIK-nya, utamanya ketika pihak asing ikut terlibat. Pejabat-pejabat Indonesia cukup menempatkan kebutuhan akan pembangunan dan pengembangan kapasitas yang berkaitan dengan keamanan siber lebih tinggi daripada risiko menggunakan hardware TIK China dalam sistem infrastruktur kritis mereka.

Jika negara-negara demokrasi liberal yang kaya prihatin dengan tren demikian, maka mereka perlu menawarkan alternatif yang dapat dijalankan yang menempatkan kebutuhan pengembangan digital besar Indonesia pada inti proposal dengan nilai apapun. Kecil kemungkinan bahwa Indonesia akan berhenti menggunakan hardware China dalam infrastrukturnya, namun adanya alternatif dapat mencegah ketergantungan yang berlebihan.

Pendahuluan

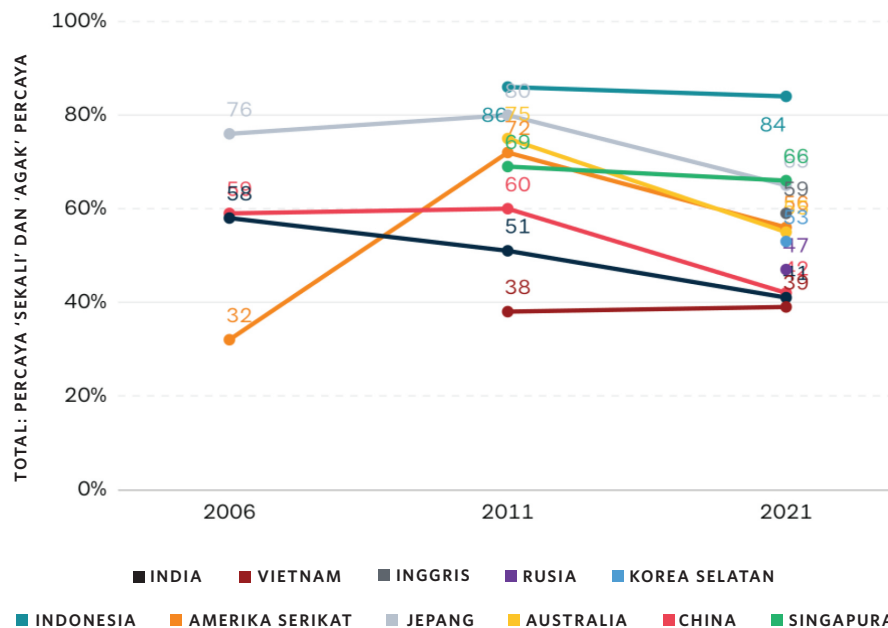
Dua tren yang tampaknya bertentangan sedang terjadi di Indonesia. Pada satu sisi, kepercayaan pada China anjlok dengan cepat (lihat gambar 1).¹ Kepercayaan pada kekuatan-kekuatan besar lainnya juga turun, tetapi China tetap jadi yang jauh lebih tidak dipercayai dibanding Amerika Serikat atau Jepang. Sumber ketidakpercayaan itu beraneka-ragam mulai dari represi China pada kaum minoritas Muslim sampai pada klaim batas maritim atas wilayah perairan yang bagi pemerintah Indonesia adalah bagian dari zona ekonomi eksklusifnya terbatasnya. Selain itu, masyarakat Indonesia mempunyai berbagai sikap pada investasi dan proyek China di Indonesia. Pabrik semen China, misalnya, dituduh memperlemah perusahaan semen lokal dan mempekerjakan pekerja-pekerja China dengan mengesampingkan warga Indonesia yang butuh pekerjaan.²

Meski ada rasa ketidakpercayaan ini, pemasok utama infrastruktur telekomunikasi buatan China di Indonesia –Huawei dan ZTE – tidak menghadapi perlawanan berarti dari pemerintah dan warga biasa Indonesia. Tak seperti beberapa jenis proyek China lainnya yang telah memicu gelombang protes di Indonesia karena lebih mendahulukan pekerja China daripada Indonesia, Huawei dan ZTE

GAMBAR 1

Menurunnya Ketidakpercayaan Indonesia pada negara Kekuatan-kekuatan Global

Seberapa jauh anda percaya negara-negara berikut agar bersikap penuh tanggung-jawab di dunia?



SUMBER: Ben Bland, Evan Laksmana, dan Natasha Kassam, "Charting Their Own Course: How Indonesians See the World," Lowy Institute, April 2022, 13, <https://interactives.lowyinstitute.org/features/indonesia-poll-2021>.

hanya mengundang pemberitaan negatif yang minim.³ Keamanan jaringan atau ancaman-ancaman potensial lain dari Huawei atau pemasok infrastruktur digital China lainnya yang mendominasi perdebatan di negara lain ternyata tak masuk dalam ranking teratas pada daftar panjang keprihatinan kebijakan di Indonesia.

Memang karena prioritas utama kebijakan di Indonesia adalah penciptaan lapangan kerja dan perkembangan ekonomi, maka adanya peringatan bahwa Huawei dan ZTE dapat memunculkan ancaman-ancaman keamanan pada umumnya tak cukup menggema. Seperti yang dikatakan seorang pejabat senior Indonesia pada penulis dalam sebuah wawancara: “Kalau kita terus-menerus takut, maka kita akan diam di tempat.”⁴ Upaya mengintensifkan persaingan teknologi antara China dan Amerika Serikat ataupun kasus-kasus spionase siber yang disponsori China kecil kemungkinannya akan mengubah posisi Indonesia.

Adaptasi pada kondisi lokal di Indonesia menjadi alasan utama mengapa dua eksportir hardware telekomunikasi China terbesar, Huawei dan ZTE, menjadi bagian integral dari strategi pembangunan Indonesia. Satu perbedaan harga yang menarik antara produk-produk yang mereka tawarkan dengan alternatif-alternatif produk internasional lainnya, tentu saja, adalah satu bagian dari daya tariknya.⁵ Semua orang Indonesia yang diwawancarai penulis (dari berbagai jabatan seperti di departemen dan badan pemerintah, academia, dan *think tanks*), menyatakan bahwa keuntungan harga Huawei dan ZTE merupakan faktor utama dalam keputusan Indonesia memakai peralatan China. Namun di luar keuntungan harga yang lebih rendah, Huawei dan ZTE telah berhasil dalam upaya-upaya pengembangan kapasitas yang sangat besar dan cepat berkembang bagi warga Indonesia, dan membantu mengatasi hambatan terbesar Indonesia menuju ekonomi digital yang sukses: yaitu kurangnya bakat siber keamanan dan teknologi.⁶

Kedua perusahaan China itu menawarkan pelatihan keamanan siber pada pejabat-pejabat Indonesia, pekerja-pekerja teknologi dan mahasiswa pada level yang tak tersaingi oleh perusahaan asing atau pemerintah negara lainnya. Di tahun 2020, Huawei mengklaim bahwa mereka akan melatih 100.000 warga Indonesia selama 5 tahun dalam keahlian keamanan siber.⁷ Penulis memulai riset ini dengan rasa skeptis akan jumlah sebesar itu, namun semakin kami menggali kisahnya, kami melihat adanya rejim pelatihan yang belum bisa disamai oleh perusahaan teknologi asing manapun yang beroperasi di Indonesia. Begitu kuatnya tuntutan Indonesia akan transfer pengetahuan dan keahlian, pengembangan kapasitas, dan pelatihan tenaga kerja sampai-sampai Huawei dan ZTE sendiri menghadapi perjuangan maha berat untuk mengatasi kekurangan kemampuan keamanan siber yang dihadapi Indonesia. Tetapi mereka mampu beradaptasi dengan tuntutan lokal ini dengan menawarkan lebih daripada para pesaing mereka.

Bahkan bila warga Indonesia lebih banyak mengeluh akan implikasi keamanan siber dari kemitraan erat dengan perusahaan-perusahaan telekomunikasi nasional unggulan China di tengah datangnya peringatan dari pemerintah negara-negara demokrasi kaya, Huawei dan ZTE telah menempatkan diri mereka sebagai solusi atas tantangan keamanan siber Indonesia, dan bukan sebagai sumber masalah.⁸ Dan tantangan-tantangan itu sangatlah besar. Ada 1,4 milyar serangan siber di Indonesia pada tahun 2021, naik dari jumlah 495 juta di tahun sebelumnya, menurut BSSN.⁹ Satu orang yang diwawancarai menunjukkan pada penulis bahwa pada umumnya sangat mudah untuk mengakses data pribadi seseorang di Indonesia.¹⁰ Di tengah-tengah membludaknya ancaman-ancaman siber ini, warga Indonesia dan pemerintahnya paling khawatir bukan karena China tapi tindak kriminal siber yang dilakukan oleh pemain-pemain non-negara dan ancaman-ancaman pada stabilitas sosial dan politik dalam negeri, seperti *misinformasi* dan disinformasi.¹¹ Kemungkinan spionase dan prospek pemerintah asing menggunakan infrastruktur TIK demi keuntungan maksimal sangatlah dipahami, tetapi hal ini menempati ranking yang sangat rendah dalam daftar yang perlu diperhatikan berkenaan dengan keamanan siber Indonesia.

Dengan Huawei dan ZTE menawarkan untuk membantu pejabat Indonesia untuk dapat lebih baik dalam menangkal kejahatan siber oleh pelaku non-negara, dan lebih efektif mengatur domain informasi digital, banyak pejabat di Jakarta memandang perusahaan-perusahaan ini sebagai mitra keamanan, bukan sebagai prospek antagonis.

Makalah ini pertama-tama memeriksa ekosistem TIK Indonesia dan menilai bagaimana saingan antara tuntutan perkembangan dan keamanan telah menciptakan kondisi yang tepat bagi perusahaan-perusahaan TIK China untuk berjaya. Kedua, makalah ini menganalisis sejarah Huawei dan ZTE di sektor telekomunikasi Indonesia. Ketiga, makalah ini memeriksa dimensi-dimensi kunci dari strategi lokal China: penambahan dan pengembangan kapasitas. Akhirnya, makalah ini menggali visi Indonesia terkait kepentingan keamanan siber dan bagaimana Huawei dan ZTE menemukan posisi dan dapat memenuhi visi lokal.

Tuntutan Perkembangan Indonesia

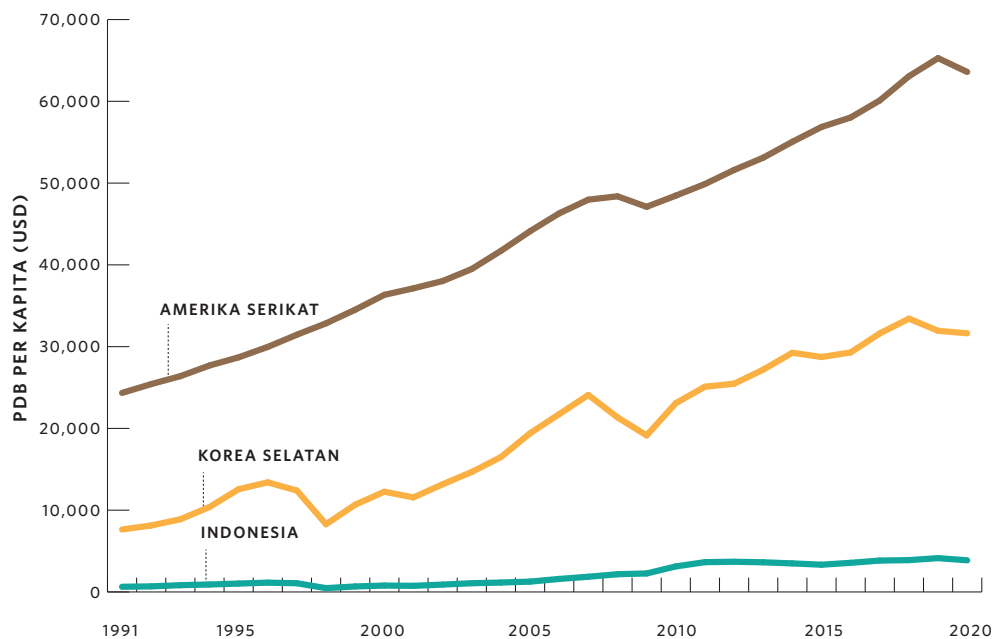
Walaupun para pembuat kebijakan di Indonesia telah memusatkan diri pada tujuan perkembangan ekonomi sejak beberapa dekade lalu, Indonesia terus menghadapi banyak tantangan sosio-ekonomi. Indonesia belum dapat menutup kesenjangan ekonomi antara dirinya dengan negara pasca-industri yang sudah maju, dan celah tersebut tambah melebar selama tiga puluh tahun silam.

Sebagai ilustrasi, gambar 2 menunjukkan celah yang makin meningkat dalam produk domestik bruto (PDB) per kapita (sesuai kurs dolar AS sekarang) antara Indonesia, Korea Selatan, dan Amerika Serikat sejak tahun 1991. Sebuah kontras terhadap argumen ini adalah bahwa PDB Amerika Serikat per kapita adalah sekitar 39 kali lebih besar daripada PDB Indonesia pada tahun 1990 tetapi kemudian turun hanya sekitar 16 kali lebih besar pada tahun 2020.¹² Namun demikian, dari sudut pandang banyak warga Indonesia, metrik statistik seperti itu tidak akan memuaskan. Cara lain untuk menyajikan data yang sama adalah dengan melihat celah yang tetap ada dalam PDB per kapita antara AS dan Indonesia – dan di situ ukuran celahnya meningkat dari \$23.710 pada tahun 1991 menjadi \$59.723 pada tahun 2020.

Para pakar ekonomi kadang-kadang lebih memilih pengukuran Keseimbangan Kemampuan Berbelanja (KKB) atau paritas daya beli dari PDB terhadap angka dalam dolar AS saat ini. Angka-angka KKB bernilai lebih rendah dalam biaya hidup dan lebih tinggi dalam keseimbangan kemampuan yang bersesuaian di negara-negara yang kurang berkembang. Sebagai contoh, biaya potong rambut, konsultasi dengan dokter, dan bahkan makanan lebih murah di Indonesia daripada barang dan jasa yang sama di Amerika Serikat. Namun, semua hardware digital kunci di Indonesia dibeli dari luar negeri, jadi bahkan kalau menggunakan angka KKB tak akan banyak memperbaiki posisi Indonesia dalam infrastruktur telekomunikasi (meskipun Indonesia punya tenaga kerja yang lebih murah untuk memasang peralatan dibanding di negara-negara maju). Ini

GAMBAR 2

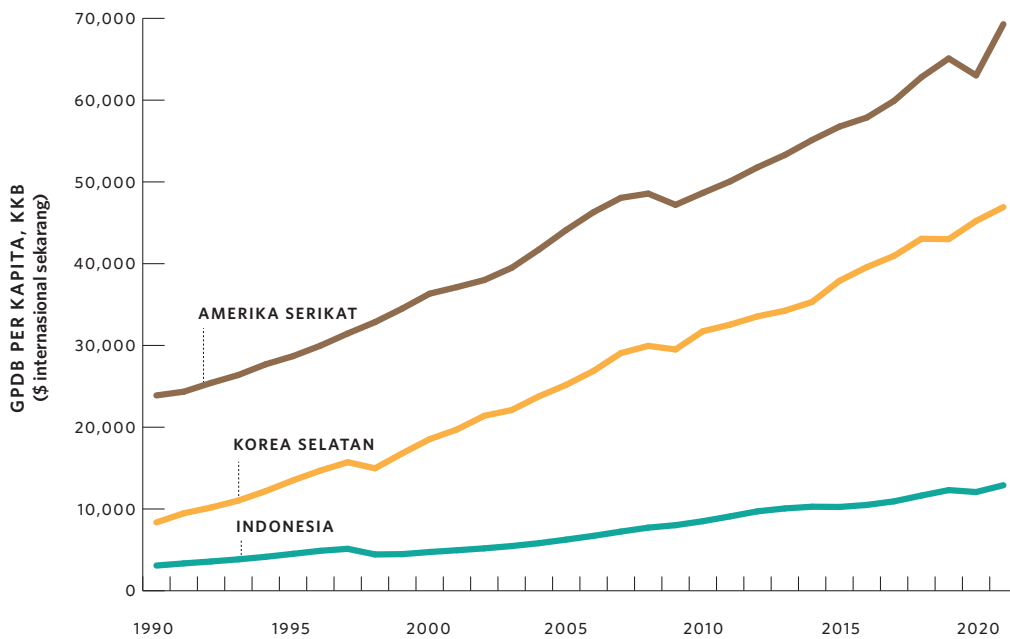
PDB Per Kapita Indonesia, Korea Selatan, dan Amerika Serikat



SUMBER: World Bank, "World Development Indicators," World Bank, 2020
<https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=US-ID-KR>.

GAMBAR 3

PDB Per Kapita yang disesuaikan Keseimbangan Kemampuan Berbelanja di Indonesia, Korea Selatan, dan Amerika Serikat



SUMBER: World Bank, "World Development Indicators," World Bank, 2020
<https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?locations=ID-US-KR>

hanyalah indikator lain yang menjadi hambatan pembangunan Indonesia: tenaga kerja murah karena kurangnya pekerjaan-pekerjaan yang berupah tinggi. Bahkan ketika pengukuran PDB Amerika Serikat, Korea Selatan, dan Indonesia disesuaikan dengan KKB (lihat gambar 3), jelas bahwa celah PDB per kapita dalam hitungan nyata (bukan kelipatan) antara Amerika Serikat dan Indonesia masihlah tumbuh dengan cepat.

Kegagalan menutup celah pembangunan ini menjadi dasar ekonomi untuk keputusan kebijakan Indonesia dalam ruang telekomunikasi dan sektor yang berkaitan dengan teknologi lainnya. Pada saat yang sama, Indonesia seperti banyak negara maju dan berkembang lain, mengalami pertumbuhan upah dan pekerjaan-pekerjaan baru terbesar dalam industri yang berkaitan dengan teknologi dan harus bergulat dengan disrupsi teknologi dalam industri-industri tradisional. Seperti yang dikemukakan oleh laporan konsultan Bain and Company pada tahun 2021, "Semakin jelaslah bahwa teknologi telah melebar jauh di luar menjadi industri itu sendiri; itulah kekuatan disrupsi utama di semua industri di dunia. Fenomena ini muncul secara empiris dalam kenyataan bahwa yang pemeroleh ekuitas terbesar di kebanyakan ekonomi global adalah perusahaan teknologi atau perusahaan dengan strategi yang dipandu teknologi."¹³ Hampir semua negara berkembang, termasuk Indonesia, sekarang menggabungkan industri teknologi sebagai komponen penting dalam jalur pembangunan mereka.

Hal itu yang memacu Indonesia untuk mengembangkan pembangunan yang berbasis digital dan teknologi-sentris. Pemerintah Indonesia berupaya menciptakan jutaan lapangan kerja tambahan di bidang ekonomi pengetahuan dan memanfaatkan digital ekonomi guna menduduki peringkat sepuluh besar ekonomi global dunia pada tahun 2030.¹⁴ Pada tahun 2021, pemerintahan Presiden Joko Widodo menyelesaikan “Roadmap Digital Indonesia 2021–2024” yang pertama. Roadmap ini tidak tersedia secara umum, namun dikabarkan bahwa roadmap itu menekankan investasi pada infrastruktur digital dan TIK, memperbaiki *human capital*, dan mengembangkan kemampuan keamanan siber yang diperlukan untuk mendukung dan melindungi ekonomi dan masyarakat yang terintegrasi secara digital.¹⁵ Roadmap ini dibangun atas prakarsa yang ada dari dekade lampau, yang menyoroti prioritas Indonesia dalam ekonomi digital dengan fokus pada kecerdasan buatan, *cloud computing*, dan 5G, serta aplikasi-aplikasi yang berkaitan dari teknologi-teknologi tersebut, termasuk untuk *smart cities*, *e-government*, dan *e-commerce* (lihat tabel 1).

TABEL 1
Kebijakan Ekonomi Digital Pemerintah Indonesia yang Terbaru

Kebijakan	Tahun	Wilayah Fokus
Roadmap E-Government Nasional ¹⁶	2016	Infrastruktur dan E-Government
Roadmap E-commerce Nasional ¹⁷	2016	E-commerce, manufaktur, ekonomi digital, dan infrastruktur
<i>Making Indonesia 4.0</i> ¹⁸	2018	Otomasi, manufaktur, dan belanja riset & pengembangan
Strategi Nasional Kecerdasan Buatan 2020–2045 ¹⁹	2020	Pelayanan kesehatan, reformasi birokrasi, keamanan pangan, mobilitas, dan <i>smart cities</i>
Roadmap Indonesia Digital 2021–2024 ²⁰	2021	Infrastruktur digital, administrasi digital, ekonomi digital, dan komunitas digital

SUMBER: berbagai sumber pemerintah dan media

Meskipun ekonomi digital Indonesia bertumbuh dengan cepat pada lima tahun kebelakang, masih saja ada kekurangan-kekurangan utama yang menghambat upaya pemerintah untuk menjadi pesaing global di bidang ekonomi digital. Pertama, Indonesia masih kekurangan talenta untuk mendukung ambisi digitalnya. Menurut sebuah laporan Bank Dunia pada tahun 2018, Indonesia menghadapi kekurangan keahlian yang serius dalam TIK dan diproyeksikan bahwa ekonomi Indonesia membutuhkan 9 juta pekerja tambahan pada tahun 2030 untuk mendukung ekonomi digital negara agar bertumbuh dengan cepat.²¹

Kedua, meskipun konektivitas digital Indonesia sudah membaik dalam dekade lampau, namun infrastruktur TIK negara tetap tak memadai untuk menghubungkan warganya sejumlah 273,5 juta

yang secara geografis terpisah-pisah.²² Juga ada masalah akses internet yang tak merata, dengan infrastruktur konektivitas yang sangat terkonsentrasi di Jawa, pulau Indonesia yang terpadat penduduknya. Pada bulan November 2020, seorang pejabat senior di Kementerian Komunikasi dan Informatika mengatakan bahwa salah satu tantangan utamanya tetap untuk menyediakan konektivitas pada sekitar 12.500 pedesaan yang tanpa akses internet.²³ Banyak desa di seluruh Indonesia harus memasang koneksi internet sendiri tanpa bantuan dari pemerintah atau swasta.²⁴

Pejabat pemerintah dan operator sistem telekomunikasi Indonesia menyadari bahwa ekspansi geografis yang cepat dan kecanggihan yang meningkat dari infrastruktur TIK-nya adalah input esensial untuk mewujudkan cita-cita menuju ekonomi digital.²⁵ Meskipun perusahaan-perusahaan TIK dalam negeri sudah mengambil tantangan untuk menghubungkan ratusan juta warga Indonesia, namun perusahaan-perusahaan itu masih membutuhkan sumber finansial yang besar dan bantuan teknis dari perusahaan asing. Namun begitu, pemerintah Indonesia menghadapi tantangan fiskal yang meningkat karena tekanan-tekanan demografinya dan kebutuhan infrastruktur yang ekstensif. Ini menimbulkan tantangan jangka panjang pada harapan Indonesia untuk memprioritaskan ekonomi digitalnya – dengan pertimbangan sifat padat modal proyek-proyek infrastruktur TIK-nya.

Infrastruktur TIK membutuhkan investasi besar dalam kabel-kabel optik fiber nasional dan internasional, *middle-mile networks*, link satelit, *shortwave radios*, dan kabel-kabel *broadband* untuk menghubungkan perumahan dan perkantoran dengan internet. Geografi Indonesia – yang terdiri dari sekitar 6.000 pulau yang dihuni – membuat infrastruktur TIK sangat padat modal.²⁶ Faktor-faktor ini telah membuat pemerintah Indonesia lebih sensitif dengan harga. Selain itu, mereka juga mengharapkan investasi asing dalam infrastruktur TIK-nya. Lebih jauh lagi, Indonesia kekurangan kemampuan dalam membangun dan memodernisasikan infrastruktur TIK sendiri. Akhirnya, Indonesia sangat bergantung pada perusahaan dan teknologi asing demi pembangunan jaringan digital yang diperlukan.

Para pimpinan politik dan pembuat kebijakan Indonesia sangat menyadari bahwa konsekuensinya sangat besar jika mereka gagal dalam menghadapi tantangan untuk mencapai transformasi digital. Indonesia telah mengalami kenaikan 25 juta pengguna internet antara tahun 2018 dan kuartal kedua tahun 2020, menjadikan Indonesia semakin dekat pada *benchmark* 200 juta pengguna internet.²⁷ Suatu laporan dari tahun 2020 tentang Asia Tenggara oleh Google, Temasek, dan Bain and Company memperkirakan bahwa nilai barang dagangan bruto di sektor e-commerce Indonesia adalah sekitar \$21 milyar.²⁸ Angka ini meningkat tajam ke \$32 milyar pada akhir 2020, dengan lebih banyak orang Indonesia berbelanja dan berbisnis online karena pandemi COVID-19.²⁹ Sementara itu, ekonomi digital Indonesia yang lebih luas bernilai \$44 milyar pada tahun 2020, dan Bain and Company memproyeksikan bahwa ekonomi digital Indonesia akan tumbuh sampai \$124 milyar

pada 2025.³⁰ Pemerintah Indonesia memperkirakan bahwa ekonomi digital akan bernilai sekitar \$146 milyar pada 2025.³¹

Di negara yang usia mediannya hanya 29 tahun, perluasan cepat internet dan ekonomi digital menjanjikan efek transformatif pada kehidupan politik, ekonomi dan sosial.³² Warga Indonesia adalah juga pengguna media sosial teraktif keempat di dunia.³³ Indonesia juga punya ekosistem startup teknologi yang dinamis dengan menghasilkan setidaknya delapan unicorn.³⁴ Didorong oleh sikap konsumen yang berubah, penetrasi telepon genggam dan internet yang cepat berkembang, sektor teknologi yang berhasil, dan kesempatan menguntungkan dalam pemasukan pajak, pemerintah melihat adanya nilai dalam mendukung transformasi digital Indonesia. Sebagai presiden, Joko Widodo telah membuat transformasi infrastruktur digital menjadi mandat nasional.³⁵ Pertumbuhan yang terus berlangsung dalam ekonomi digital merupakan tujuan sentral dalam rencana pembangunan nasional dalam beberapa dekade mendatang. Maka, tidaklah mengherankan bila baik perusahaan-perusahaan teknologi maupun modal China tertarik untuk masuk ke pasar Indonesia mengingat statusnya yang berpotensi sebagai salah satu ekonomi digital terbesar di dunia.³⁶

Peran Huawei dan ZTE dalam Infrastruktur Digital Indonesia

Huawei dan ZTE merupakan perusahaan manufaktur peralatan orisinal yang memproduksi infrastruktur dan hardware untuk operator jaringan (juga disebut *telcos* atau *carriers*). Operator-operator menjual jasa pada konsumen menggunakan infrastruktur yang disediakan oleh para perusahaan manufaktur. Di Indonesia operator jaringan adalah perusahaan-perusahaan Indonesia sendiri.

Menyediakan infrastruktur pada operator jaringan bukanlah satu-satunya lini bisnis Huawei dan ZTE di Indonesia. Huawei khususnya memiliki jangkauan aktivitas bisnis yang luas. Aktivitas ini bisa dipisahkan menjadi tiga kategori (lihat tabel 2). Huawei memanufaktur dan menjual alat-alat pribadi seperti telepon pada konsumen. Mereka juga menyediakan solusi hardware dan software pada perusahaan besar dan organisasi besar lainnya, seperti universitas dan pemerintah daerah. Bisnis *carrier* Huawei juga menyediakan peralatan jaringan untuk perusahaan-perusahaan *carrier* Indonesia.

Pada tingkat global (termasuk China), Huawei adalah *market leader* berdasarkan pendapatan dalam bisnis peralatan perusahaan *carrier*, sementara ZTE adalah pemain biasa (lihat gambar 4). Namun, China sebagai rumah pasar dua perusahaan tersebut, bernilai sekitar seperempat dari pasar peralatan perusahaan *carrier* global.³⁹ Di luar China, pangsa pasar Huawei lebih dekat pada pangsa pasar Nokia dan Ericsson (lihat gambar 5). Sedangkan ZTE merupakan pemain yang relatif kecil di luar China dalam segmen pasar ini. Makalah ini berfokus pada bisnis *carrier* Huawei dan ZTE di Indonesia,

TABEL 2

Wilayah Bisnis Huawei dan ZTE

Wilayah Kerja	Definisi	Pesaing Huawei dan ZTE
Bisnis Konsumen	Produksi barang konsumen seperti telepon, tablet, dan laptop	Apple, Samsung, Tecno, dan Oppo
Bisnis <i>carrier</i>	Membangun dan mengatur peralatan jaringan, seperti tower base station, kabel, dan lisensi alat-alat Long Term Evolution (LTE) ³⁷	Ericsson, Nokia, Alcatel-Lucent, dan Siemens
Bisnis perusahaan	Software privat yang dibuat menurut klien yang melibatkan informasi eksklusif untuk pesan instan perusahaan dan fungsi-fungsi lain ³⁸	Cisco dan IBM

SUMBER: Henry Tugendhat, "How Huawei Succeeds in Africa: Training and Knowledge Transfers in Kenya and Nigeria," China-Africa Research Initiative, kertas kerja 34, Maret 2020, 5, <https://static1.squarespace.com/static/5652847de4b033f56d2bdc29/t/5e73acb2efefbe3e97b7c258/1584639155488/WP+34+-+Tugendhat+-+Huawei+Kenya+Nigeria.pdf>.

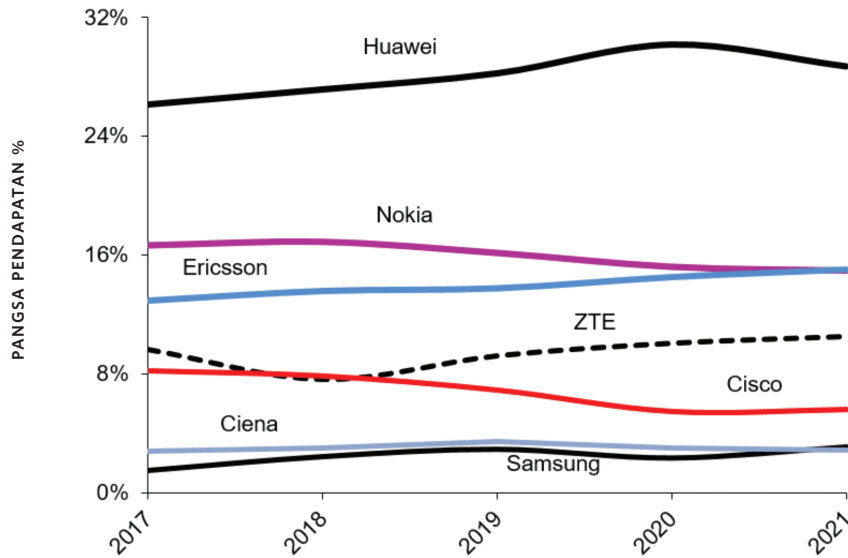
di mana ini bisnis mereka mencakup piranti keras dan lunak utama yang digunakan oleh pemerintah. Sedangkan bisnis konsumen kedua perusahaan tidak akan di bahas pada laporan ini.

Lebih sulit memastikan pangsa pasar perusahaan China di pasar peralatan *carrier* telekomunikasi Indonesia. Namun bukti yang ada menunjukkan bahwa Huawei menduduki peringkat pertama. Semua orang yang kami wawancarai mengatakan bahwa Huawei adalah pemasok terbesar.⁴⁰ Sebuah laporan riset privat yang didapat dari sebuah perusahaan bernama 6WResearch menyatakan bahwa Huawei memiliki 31,7 persen pangsa pasar, sedangkan Nokia di peringkat dua dengan 14,6 persen pada tahun 2021.⁴¹ Pada umumnya Huawei cenderung lebih bagus di negara berkembang. Penulis mengirim email pada Huawei di Indonesia dengan sejumlah pertanyaan termasuk berapa pangsa pasar Huawei. Huawei tidak memberikan detil spesifik, tetapi mencatat skala kurangnya Indonesia dalam infrastruktur TIK dan keahlian digital dan selanjutnya mendorong Huawei untuk membantu Indonesia memenuhi kebutuhannya.⁴²

Perusahaan-perusahaan China tak selalu menjadi penyedia peralatan telekomunikasi yang dominan di Indonesia. ZTE membuka bisnis mereka di Indonesia pada tahun 1999, melalui pendirian cabang di Jakarta.⁴³ Sementara itu, Huawei masuk ke pasar Indonesia pada tahun 2000 melalui pendirian anak cabangnya.⁴⁴ Masuknya mereka ke pasar Indonesia terjadi pada saat tingginya kompetisi di sektor telekomunikasi. Setelah beberapa dekade di bawah kendali negara yang kuat, sektor telekomunikasi Indonesia mengalami reformasi yang ekstensif pada awal '90-an untuk menarik modal asing dan keahlian lebih banyak agar dapat dengan cepat menumbuhkan infrastruktur komunikasi Indonesia. Menjelang pertengahan '90-an, operator telekomunikasi Indonesia sudah mengamanakan *joint venture* dengan, antara lain, France Telecom, Telstra Global, NTT Communications,

GAMBAR 4

Pendapatan Peralatan Telekomunikasi Seluruh Dunia oleh Perusahaan Manufaktur Peralatan Orisinal

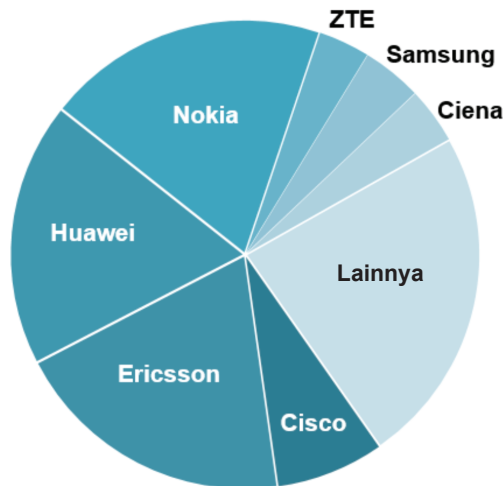


Dell'Oro Group (2021)
"Peralatan meliputi: akses broadband, transportasi microwave dan optik,
Mobile Core Network & RAN, SP Routers & Switch

SUMBER: Stefan Pongratz, "Key Takeaways - 2021 Total Telecom Equipment Market," Dell'Oro Group, Maret 14, 2022 <https://www.delloro.com/key-takeaways-2021-total-telecom-equipment-market>

GAMBAR 5

Pendapatan Peralatan Telekomunikasi Seluruh Dunia di luar China oleh Perusahaan Manufaktur Peralatan Orisinal



Dell'Oro Group (2021)
"Peralatan meliputi: akses broadband, transportasi microwave dan optik,
Mobile Core Network & RAN, SP Routers & Switch

SUMBER: Stefan Pongratz, "Key Takeaways - 2021 Total Telecom Equipment Market," Dell'Oro Group, Maret 14, 2022, <https://www.delloro.com/key-takeaways-2021-total-telecom-equipment-market>.

dan Singapore Telecom.⁴⁵ Sektor ini malah jadi makin jenuh dengan adanya perusahaan-perusahaan telekomunikasi dalam dan luar negeri menyusul krisis keuangan Asia tahun 1997–1998, selagi sektor ini mendapat tekanan keras untuk melakukan deregulasi sebagai syarat pinjaman dari International Monetary Fund (IMF). Lebih jauh lagi, deregulasi juga membuat operator telekomunikasi Indonesia punya otonomi lebih untuk beroperasi dengan perusahaan-perusahaan asing dan bereksperimen dengan lebih banyak teknologi komunikasi.⁴⁶

Meskipun ada penurunan dalam daya beli konsumen, berakhirnya krisis finansial Asia disusul oleh periode meningkatnya pemakaian internet, yang ditandai juga dengan munculnya rezim demokratis baru – dan berakhirnya rezim otoriter Orde Baru -. Meskipun diperkirakan hanya ada 700.000 pengguna internet aktif pada tahun 1997, lebih dari 4 juta orang Indonesia sudah bisa online pada tahun 2001 dan 2002.⁴⁷ Dalam upaya memenuhi tuntutan pemakaian internet yang makin meningkat, operator-operator telekomunikasi Indonesia meluncurkan rencana berskala besar untuk memperluas jangkauan jaringan seluruh negeri. Huawei dan kemudian ZTE bergabung dengan sekelompok perusahaan-perusahaan TIK asing untuk bersaing untuk memenangkan bagian dari bisnis peralatan telekomunikasi Indonesia yang dinamis dan makin luas.

Pada bulan Juni 2003, Huawei berhasil mengamankan kemitraannya yang pertama di Indonesia melalui kontrak senilai \$10 juta dengan PT Excelcomindo Pratama (kini XL) untuk memasok peralatan GSM yang diperlukan dalam memperluas jaringan operator tersebut di Sumatra, Kalimantan, dan Sulawesi.⁴⁸ Sementara itu, ZTE berhasil mengamankan proyek pertamanya pada bulan Juli 2004, ketika diberi kontrak senilai \$47,6 juta untuk membantu Telkom Indonesia membangun jaringan CDMA dan jaringan *digital loop carrier* yang menghubungkan Jakarta dan wilayah-wilayah sekitarnya.⁴⁹

Keberhasilan kedua perusahaan ini diikuti oleh serangkaian kontrak utama yang terus mengalir dari pemerintah dan perusahaan telekomunikasi Indonesia untuk Huawei dan ZTE, kadang-kadang bekerjasama dengan perusahaan TIK asing lainnya, untuk mengembangkan jaringan seluler dan infrastruktur telekomunikasi Indonesia. Dari tahun 2009, anak cabang Huawei, Huawei Marine, berhasil memenangkan sederet kontrak bernilai besar untuk membantu konstruksi sistem kabel bawah laut yang memperbaiki penetrasi internet dan konektivitas di Barat Laut Indonesia.⁵⁰ Sementara itu, ZTE menjadi pemasok peralatan besar untuk perusahaan-perusahaan telekomunikasi Indonesia dalam upaya membangun jaringan 3G dan 4G/LTE.⁵¹

Pada awal 2010, Huawei dan ZTE menawarkan jasa lebih banyak di luar konstruksi jaringan telekomunikasi yang mencakup jasa yang bertujuan untuk memenuhi tujuan pemerintah Indonesia dalam mendigitalkan ekonomi dan pemerintahan. Melalui program *Smart City*, Huawei dan perusahaan-

perusahaan telekomunikasi Indonesia menyediakan jasa digital, infrastruktur keamanan publik, dan pembangunan keamanan siber dan kapasitas teknis pada beberapa pemerintah kotamadya Indonesia. ZTE menyediakan jasa ini pula. Pada bulan Agustus 2005, ZTE menandatangani MoU dengan pemerintah kota Makassar guna memperbaiki sistem keamanan umum, termasuk melalui penggunaan teknologi pada pekerja kedaruratan agar bisa berkomunikasi dan memberi respon terhadap krisis secara cepat.⁵² Huawei juga membangun pusat riset di Jakarta yang berfokus pada pengembangan software.⁵³

Keberhasilan Huawei dan ZTE, termasuk di Indonesia, sering diakibatkan pada kemampuan dalam memanfaatkan harga produk mereka yang rendah. Meskipun sulit untuk memperoleh angka yang pasti, para pengamat industri dan pejabat pemerintah berulang kali mengatakan bahwa harga produk Huawei dan ZTE yang lebih murah setidaknya menjelaskan melejitnya mereka sebagai penyedia TIK utama di Indonesia.⁵⁴ Pada awalnya, penghematan biaya tersebut mungkin disebabkan oleh banyaknya tenaga kerja teknis China yang upahnya rendah, sehingga membuat mereka bisa bersaing dengan saingan mereka.⁵⁵ Namun begitu, sekarangpun ketika upah China sudah meningkat banyak dan pengeluaran penelitian dan pengembangan Huawei telah berlipat ganda, para ahli yang kami wawancarai menyatakan bahwa Huawei dan ZTE dapat menawarkan harga yang lebih rendah daripada pesaing-pesaing mereka. Ini konsisten dengan investigasi yang dilakukan *Wall Street Journal* pada tahun 2019 yang mendukung penemuan bahwa Huawei mampu memberi pilihan pendanaan yang sangat kompetitif dan mengalahkan pesaing-pesaing mereka dalam hal harga sampai sekitar 30%.⁵⁶ Investigasi ini menemukan bahwa Huawei dapat mengalahkan saingan mereka seperti Ericsson dan Nokia karena dukungan pendanaan sebesar puluhan milyar dolar dari pemerintah China selama lebih dari dua dekade.⁵⁷

Keuntungan pemakaian produk Huawei dan ZTE tidak saja karena harganya mereka yang lebih rendah. Bank-bank BUMN China -baik *policy bank* maupun bank komersial- telah berjanji untuk menyediakan setidaknya \$600 juta sebagai bantuan finansial dalam *export buyer's credit* ke perusahaan-perusahaan Indonesia pada tahun 2005 dan 2007, yang mungkin ikut membantu perusahaan telekomunikasi Indonesia dapat membeli produk-produk Huawei dan ZTE.⁵⁸ Pada bulan Agustus 2010, Industrial and Commercial Bank di China, yakni bank BUMN China terbesar, menandatangani perjanjian *export buyer's credit* dengan klien-klien Huawei di Indonesia untuk mendanai impor produk-produk Huawei.⁵⁹ Pada bulan November 2017, China Development Fund (yayasan investasi dari China Development Bank, salah satu dari dua pemberi pinjaman polis utama Beijing) juga memberikan kredit pada PT Global Mediacom untuk membeli produk-produk ZTE.⁶⁰

Meski pun harga mereka sudah lebih rendah, Huawei dan ZTE juga menawarkan produk-produk tambahan, yang dapat dibagi dalam dua kategori. Yang pertama adalah tambahan (*add-ons*) untuk

produk-produk – seperti pemeliharaan dan dukungan teknis di samping pelatihan yang lebih baik pada mereka yang menggunakan teknologi mereka. Gerald F. Rossi, yang bertindak sebagai Presiden Direktur Excelcom ketika Huawei diberi kontrak Indonesia pertamanya, mengaitkan keberhasilan Huawei pada “komitmen akan standard tinggi dukungan jasa dan *pelatihan lokal*.”⁶¹ Pada khususnya, Huawei dan ZTE dapat menang gerak atas para pesaingnya dengan cara menyediakan jasa bantuan teknis (termasuk pemeliharaan) dan berinvestasi dalam pelatihan.

Tawaran tambahan kedua itu adalah komitmen luas dalam mengembangkan kapasitas teknologi dan modal manusia di Indonesia. Seiring berjalannya waktu, Huawei dan ZTE menjadi semakin paham seberapa pentingnya pengembangan kapasitas merupakan prioritas pemerintah Indonesia. Pada bulan Mei 2006, ZTE membuka pusat pelatihan telekomunikasi dalam kemitraan dengan Institut Teknologi Telkom (sekarang Universitas Telkom).⁶² Huawei membangun pusat riset dan pelatihan untuk membantu mengembangkan keahlian tenaga kerja yang diperlukan demi kebutuhan perusahaan Huawei sendiri, serta juga untuk membantu pembangunan modal manusia TIK Indonesia secara keseluruhan. Pada bulan April 2011, Huawei mendirikan pusat pelatihan TIK dengan Institut Teknologi Bandung, yang melatih mahasiswa dan peneliti Indonesia tentang protokol-protokol internet.

Badan-badan pemerintah Indonesia juga menjadi penerima program pelatihan yang dirancang oleh Huawei. Pada bulan Januari 2016, Badan Pengkajian dan Penerapan Teknologi (BPPT), badan pemerintah yang kini tak beroperasi namundulu bertugas membuat riset mengenai penerapan teknologi baru, menandatangani perjanjian dengan Huawei agar perusahaan itu membantu mengembangkan kapasitas BPPT untuk merencanakan aplikasi kecerdasan buatan dan cloud computing untuk tujuan-tujuan pemerintah dan ekonomi digital. Pada bulan Oktober 2019, Huawei menandatangani persetujuan dengan BSSN untuk membantu mengembangkan modal manusia melalui pelajaran-pelajaran lanjutan tentang keamanan siber. Persetujuan ini diperbarui pada bulan September 2021 (meskipun tidak jelas apakah ini berbeda artinya dalam praktiknya).⁶³ Bagian berikut makalah ini akan melihat secara rinci ukuran program pelatihan Huawei yang makin besar dengan cepat di Indonesia.

Strategi-strategi Huawei dan ZTE untuk menjadi perusahaan telekomunikasi yang dominan di Indonesia berjalan baik. Seperti disebut di muka, Huawei dan ZTE merupakan pemain utama di sektor peralatan carrier Indonesia dan sektor bisnis peralatan perusahaan. Lebih jauh lagi, Huawei dan ZTE telah melakukan kerjasama dengan operator-operator telekomunikasi utama Indonesia untuk membangun jaringan mobile 5G Indonesia karena perusahaan-perusahaan ini menghadapi tantangan besar di banyak negara maju.⁶⁴ Walaupun di Indonesia masih ada persepsi negatif tentang China, namun Huawei dan ZTE belum mengundang protes besar atau meluas di media. Nyatanya, peran mereka malah dilihat secara positif di banyak bagian masyarakat Indonesia.

Pelatihan dan Pengembangan Kapasitas

Peran China dalam pelatihan dan meningkatkan keterampilan teknologi digital warga Indonesia kebanyakan digerakkan oleh perusahaan. Perusahaan-perusahaan merespon pada tuntutan dari bagian pemerintah atau masyarakat Indonesia, karena mereka menyadari perlunya lisensi sosial untuk beroperasi. Indonesia kekurangan kepakaran TIK dan wirausahawan yang paham teknologi. Seperti yang dinyatakan dalam suatu laporan pemerintah Australia, “Indonesia hanya punya 278 pekerja TI per 1 juta penduduk, dibanding Malaysia (1.834) dan India (1.159)”⁶⁵ Sebagai tambahan, perusahaan-perusahaan TIK telah menyatakan kebutuhan akan lulusan yang jauh lebih berkualitas daripada yang dihasilkan oleh sistem pendidikan Indonesia.⁶⁶

Janji Huawei untuk menyediakan pelatihan pada warga Indonesia dalam teknologi TIK tak tersaingi dan merupakan nilai jual utama perusahaan itu. Komitmen-komitmen ini meningkat seiring waktu, termasuk janji untuk melatih 100.000 warga Indonesia pada tahun 2020.⁶⁷ Tabel 3, di bawah, menunjukkan contoh janji pelatihan dari perusahaan-perusahaan TIK China sampai tahun 2021. Karena begitu banyak janji telah dibuat, sulitlah untuk mengartikan janji mana yang dipenuhi dengan terlaksananya pelatihan. Tetapi Huawei melatih ribuan, dan mungkin sekali puluhan ribu, warga Indonesia tiap tahunnya. Di luar contoh-contoh yang ada dalam tabel 3, perusahaan-perusahaan China juga menyediakan pelatihan yang lebih kecil dan tidak diformalkan, termasuk *on-site job training* atau interaksi-interaksi skala kecil seperti pelatihan keamanan siber yang ditawarkan Huawei pada BSSN pada bulan November 2021.

TABEL 3

Contoh Pelatihan TIK yang Dijanjikan oleh Huawei dan ZTE di Indonesia

Perusahaan China	Waktu	Detil
Huawei	Januari 2011	Huawei meluncurkan program “Seeds for Future” untuk mahasiswa TIK Indonesia dimana mereka menerima pelatihan TIK, beasiswa, dan kesempatan magang. ⁶⁸ Proyeknya berjalan online pada 2021 karena pembatasan perjalanan yang berkaitan dengan pandemi di China. ⁶⁹
Huawei	April 2011	Huawei mendirikan Pusat Pelatihan dengan Sekolah Teknologi di ITB. ⁷⁰
Huawei	Maret 2017	Huawei meluncurkan SmartGen, program pelatihan TIK untuk mahasiswa tujuh universitas top. ⁷¹
Huawei	Januari 2019	Huawei menandatangani MoU untuk membantu modal manusia di BSSN. ⁷² MoU diperbarui pada 2021. ⁷³
Huawei	Januari 2020	Huawei berjanji melatih 100.000 orang dalam teknologi digital, seperti cloud computing dan 5G. ⁷⁴
Huawei	Januari 2021	Huawei membuka Huawei-ASEAN Academy Engineering Institute, berkolaborasi dengan beberapa universitas terkemuka Indonesia. ⁷⁵ Dekan Akademi memperkirakan bahwa “1.500-2.000 pelatihan & program sertifikasi TIK . . . dapat diselesaikan tiap tahun.”
ZTE	Juni 2021	ZTE mendirikan Pusat Pelatihan Teknik & Servis. ⁷⁶ Sangat sedikit detil tersedia tentang jumlah mahasiswa yang disasar.

SUMBER: Berbagai sumber perusahaan dan media.

Perusahaan-perusahaan TIK China tidak selalu memenuhi komitmen pelatihan mereka. Sebagai contoh, ZTE mendirikan pusat pelatihan di STT Telkom (institusi pelatihan telekomunikasi) pada tahun 2006.⁷⁷ ZTE pada awalnya mengklaim bahwa mereka pada akhirnya akan melatih 10.000 mahasiswa per tahun (sebuah komitmen yang tak tertulis dalam daftar di atas dikarenakan sifat historisnya). Meskipun pusat itu tetap terus berjalan, tak ada indikasi mereka telah beroperasi pada skala yang dibayangkan. Serupa dengan itu, pada tahun 2018, Jack Ma, pendiri perusahaan teknologi China Alibaba Group, menyatakan bahwa dia berencana membuka institusi pelatihan bagi wirausahawan di Indonesia (sebuah prakarsa yang tak tercantum dalam daftar di atas karena pengumuman ini tak mencakup suatu penanda-tanganan formal atau pembukaan sebuah pusat pelatihan).⁷⁸ Penulis makalah ini tak dapat menemukan informasi lebih jauh di luar pengumuman awal itu, yang dapat mengindikasikan bahwa institusi itu tak pernah menjadi kenyataan.

Meskipun ada kekurangan-kekurangan ini, Huawei dan ZTE mengeluarkan banyak sumber daya untuk meningkatkan kemampuan TIK warga Indonesia. Pelatihannya tidak saja untuk karyawan-karyawan mereka sendiri. Huawei, sebagai contoh, memberikan pelatihan bagi pegawai pemerintah, mahasiswa universitas, dan mereka yang ingin menambah kemampuan atau berganti karier juga. Hampir di setiap bulan, besar kemungkinan muncul laporan tentang program kursus pelatihan Huawei yang menargetkan pegawai negeri Indonesia. Huawei mengklaim sudah mengadakan bermacam-macam “kegiatan pelatihan atau webinar” dan kegiatan-kegiatan pembangunan kapasitas “untuk hampir 7.000 pegawai pemerintah (Indonesia) sejak tahun 2019.”⁷⁹ Namun, kualitas tawaran-tawaran tetaplak tak jelas. Ini hanyalah satu program pemerintah dari banyak program yang dijanjikan oleh Huawei.

Di luar program-program pelatihan itu, Huawei menyediakan kursus-kursus jangka pendek gratis atau bersubsidi untuk mengembangkan keahlian dalam *software development* dan membantu meningkatkan keahlian di bidang *hardware* di tingkat universitas dan perguruan tinggi pelatihan. Onno W. Purbo, spesialis TI Indonesia yang terkemuka dan seorang akademisi, menunjukkan pada penulis sebuah email dari Huawei yang menawarkan pemberian sertifikat internasional gratis selama lima minggu dalam pengembangan aplikasi pada mahasiswa di Institut Teknologi Tangerang Selatan. Apple menawarkan kursus pengembangannya sendiri di Indonesia. Beberapa kursus ini gratis, seperti yang ditawarkan di Universitas Binus.⁸⁰ Tapi tampaknya jauh lebih sedikit yang diterima daripada yang ditawarkan Huawei. Di luar program-program ini Apple juga mengadakan program berbayar.⁸¹ Purbo menyatakan ini akan jadi halangan buat banyak mahasiswanya.⁸² Purbo menerima tawaran Huawei karena memberikan jalan gratis pada para mahasiswanya pada kesempatan pekerjaan yang lebih baik. Kursus pelatihan berjalan pada bulan Maret 2022. Purbo memperkirakan kalau lebih dari 1.000 mahasiswa ikut serta dalam pelatihan itu. Email tersebut juga menanyakan kalau dia bisa memperkenalkan Huawei pada universitas lain di Indonesia.⁸³ Ini mengindikasikan bahwa Huawei secara aktif mencari kesempatan-kesempatan pelatihan bagi warga Indonesia di Indonesia,

termasuk di pedesaan. Tak satupun dari prakarsa ini dicatat dalam pengumuman tingkat atas, dan cenderung tak terdengar suaranya.

Mayoritas pekerja yang direkrut Huawei dan ZTE di Indonesia adalah tenaga-tenaga lokal. Sebuah artikel di *Jakarta Post* tahun 2021 menyatakan bahwa tenaga lokal menyumbang sekitar 90 persen dari lebih 2.000 pekerja di seluruh Indonesia.⁸⁴ Banyak orang yang diwawancarai di kalangan pemerintahan, akademisi, dan bisnis sependapat kalau Huawei merekrut tenaga lokal.⁸⁵ Tak satupun dari mereka menyatakan keprihatinan akan kurangnya tenaga lokal. Pencarian penulis makalah di pemberitaan media Indonesia menunjukkan bahwa tenaga kerja China yang bekerja di proyek-proyek China merupakan keprihatinan bersama, namun jarang pekerja China yang melibatkan Huawei dan ZTE menjadi isu politik kontroversial di negara ini.

Di luar pernyataan umum tentang keinginan untuk mendorong kemampuan keamanan siber Indonesia, Huawei dan ZTE tak terang-terangan menyatakan mengapa mereka mendanai kesempatan-kesempatan pelatihan yang begitu beraneka tersebut di Indonesia, sampai pada tingkat di luar apa yang penting bagi proyek mereka sendiri. Pernyataan umum itu menjelaskan tidak juga mengapa upaya-upaya pelatihan TIK telah meningkat besar-besaran dalam tahun-tahun terakhir.

Berdasar pada wawancara dengan pejabat dan spesialis keamanan siber Indonesia, penulis memperkirakan tiga alasan.⁸⁶ Pertama, penting bagi kedua perusahaan untuk mendapatkan kontrak sosial untuk beroperasi di Indonesia. Mereka sadar akan kewaspadaan global pada China dan perusahaan-perusahaan teknologi China. Kedua perusahaan perlu menunjukkan bahwa mereka menawarkan nilai pada komunitas di negara tuan rumah.

Kedua, melatih warga lokal adalah cara terbaik untuk mendapatkan konsumen. Ketika penulis bertanya pada Purbo mengapa Huawei memberikan pelatihan pada mahasiswanya, jawabannya “Karena mereka ingin kita membeli produknya.”⁸⁷ Warga lokal yang menerima pelatihan dapat pergi bekerja di tempat yang berpotensi menjadi client Huawei atau ZTE, seperti bank, universitas, dan departemen pemerintah. Jika dan ketika mereka melakukan hal demikian, mereka sudah akan punya pengetahuan dan hubungan dengan Huawei. Henry Tugendhat memiliki temuan yang sama pada makalah riset tentang Huawei di Kenya dan Nigeria. Seorang jurubicara Huawei dikutip sebagai berikut dalam makalah tersebut: “Kami melatih mahasiswa-mahasiswa universitas dengan harapan mereka akan jadi konsumen di masa depan, seperti di Cisco. Sekarang kami menawarkan pelatihan ini secara gratis pada universitas-universitas, meskipun para mahasiswa masih harus membayar sejumlah biaya ke universitas mereka sebagai bagian dari biaya kuliah mereka. Kami bermaksud kualifikasi dari kami setara dengan sertifikasi pegawai sehingga program ini bisa berfungsi sebagai mata kuliah pilihan atau bagian dari tugas mata kuliah mereka, sebagai contoh.”⁸⁸

Ketiga, Huawei dan ZTE dapat juga mengatakan pada pemerintah China bahwa pelatihan yang mereka berikan bisa meningkatkan penyerapan teknologi China oleh negara lain, yang merupakan tujuan politis kunci bagi pemerintah China. Huawei menerima sejumlah besar pendanaan negara yang bersubsidi, dan kemungkinan perlu mendemonstrasikan kalau mereka betul-betul menyampaikan hasil politis bagi para pemimpin di Beijing.

Huawei, serta juga ZTE namun dalam skala yang lebih kecil, telah melaksanakan banyak upaya pada pelatihan dan pengembangan kapasitas dalam sektor TIK. Belakangan pemerintah China mulai mengetes program peningkatan kemampuan dan pelatihannya sendiri pada warga yang tinggal di negara berkembang, termasuk Indonesia. Banyak pejabat sudah lama membicarakan tentang program pendidikan kejuruan global yang diberikan oleh China. Sebagai contoh, pada tahun 2011, perdana menteri saat itu Wen Jiabao menyampaikan proposal bahwa China “mendirikan sepuluh pendidikan kejuruan dan pusat pelatihan untuk membantu negara-negara ASEAN mengembangkan SDM yang dibutuhkan dalam pengembangan ekonomi dan sosial.”⁸⁹ Namun, sampai belum lama lewat, pemerintah China menawarkan hanya sedikit program untuk pelatihan kejuruan di luar negeri.

China berada dalam tahap awal mendirikan sekolah tinggi kejuruan yang dinamakan Luban Workshops di puluhan negara untuk melatih mahasiswa dalam mata kuliah seperti TIK.⁹⁰ Program-program pelatihan kejuruan ini berasal dari sebuah proposal pemerintah lokal. Program pertama dibentuk di Thailand pada tahun 2016 oleh pemkot Tianjin (tempat asal Lu Ban). Sejauh ini, dilaporkan mereka telah melatih lebih dari 1,000 mahasiswa Thai dan lebih dari 8.000 murid dari negara-negara lain di Asia Tenggara, kemungkinan juga termasuk Indonesia.⁹¹

Luban Workshops umumnya di selenggarakan oleh institusi lokal di negara yang berpartisipasi, seringkali di sekolah-sekolah tinggi kejuruan. Pada bulan Mei 2021, sebuah surat kabar harian di China mengabarkan bahwa sebanyak 18 workshop sudah didirikan di penjuru dunia.⁹² Pejabat pemerintah China menjanjikan bahwa pada bulan September setidaknya sepuluh workshop akan didirikan di negara-negara anggota Shanghai Corporation Organization, dengan potensi tumpang tindih dengan rencana-rencana sebelumnya. Kemudian Tianjin Dongli District Vocational Education School mendirikan Luban Workshop pertamanya di Indonesia pada bulan November 2017.⁹³ Pada workshop ini, para siswa belajar keterampilan TIK dan lainnya. Ada kemungkinan lebih banyak workshop akan didirikan di Indonesia.

Pemerintah China juga membuat upaya lain untuk meningkatkan keterampilan para pekerja dan mentransfer teknologi pada Indonesia. Banyak dari prakarsa ini diawali di tingkat provinsi. Hasil dari program *outreach* ini belum meyakinkan. Guanxi Zhuang Autonomous Region telah mencoba memosisikan diri sebagai pusat utama teknologi dan pertukaran pelatihan ASEAN-China. Fungsionalitas program ini pun belum jelas.

China dan Indonesia juga mendirikan pusat transfer teknologi di Guangxi, yakni yang kelima antara China dan sebuah negara ASEAN.⁹⁴ Pusat-pusat transfer teknologi ini didirikan dalam naungan *China-ASEAN Technology Transfer Center* yang lebih luas.⁹⁵ Tampaknya pusat-pusat ini sedikit dalam realitanya. Situs webnya pun hanya memberikan sedikit informasi baru sejak tahun 2015. China-ASEAN Cybersecurity Exchange and Training Center didirikan di Nanning, Guangxi, pada tahun 2019.⁹⁶ Pusat ini masih pada tahap awal pengembangan. Dan sementara negara-negara lain menaruh investasi pada pendidikan kejuruan teknis di Indonesia, tak ada satupun negara yang bisa menyamai janji Huawei untuk melatih 100.000 mahasiswa di sektor TIK.⁹⁷

Visi Lain dalam Keamanan

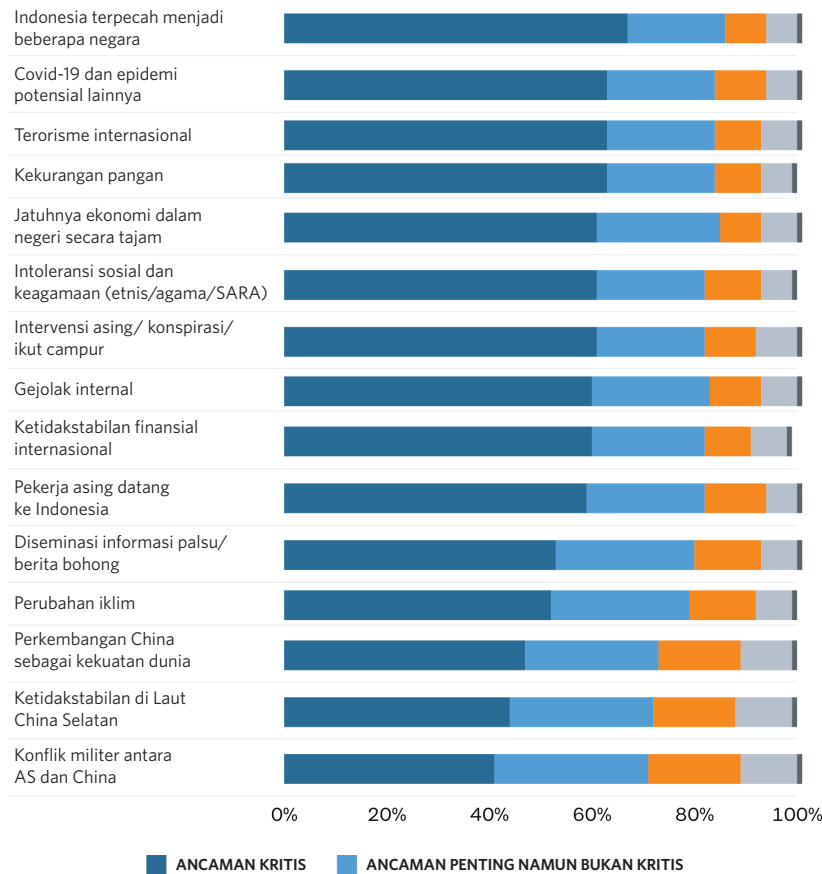
Warga Indonesia punya keprihatinan serius tentang China, namun keraguan ini bukanlah yang teratas dalam daftar panjang tantangan potensial bagi negara Indonesia. Sebuah polling yang diadakan oleh Lowy Institute pada tahun 2021 meminta warga Indonesia untuk membuat ranking berbagai jenis ancaman (lihat gambar 6).⁹⁸ Jawaban yang datang yang secara langsung menyebut China ternyata dilihat sebagai yang paling rendah mengancam. Ini adalah daftar relatif, dan banyak responden prihatin ancaman yang melibatkan China seperti perang AS-China, perselisihan di Laut China Selatan, dan bangkitnya China. Namun ini semua dilihat sebagai ancaman yang lebih rendah dibanding terorisme, ketidak-stabilan dalam negeri, dan kekurangan pangan, ditambah banyak isu lainnya. Isu pekerja asing (yang juga mencakup China) dilihat sebagai ancaman yang lebih besar daripada konflik AS-China dan Laut China Selatan.

Pandangan-pandangan ini mengalir ke dalam bagaimana Indonesia memperlakukan keterlibatan keamanan sibernya dengan China. Perkembangan digital Indonesia utamanya tentang pekerjaan dan pertumbuhan ekonomi. Resiko keamanan siber yang terbesar dari perspektif pemerintah adalah bahwa lingkungan online-nya tidak cukup kompetitif untuk menciptakan pekerjaan yang memadai atau lingkungan keamanan sibernya terlalu tak aman untuk dipercayai oleh warga Indonesia. Walaupun ada pengakuan atas aktivitas siber berbahaya China, resiko-resiko yang berkaitan dengan itu tidaklah termasuk dalam ranking tinggi dibanding sederetan tantangan-tantangan keamanan lainnya yang lebih mendesak.⁹⁹

Buku Putih Pertahanan Indonesia tahun 2008 merupakan buku putih pertama yang mengenali kerentanan-kerentanan keamanan siber. Dokumen tersebut melihat bahwa kelemahan sistem siber Indonesia terhadap kejahatan kriminal siber tumbuh seiring ukuran basis pengguna internet dan telepon genggam.¹⁰⁰ Ancaman lain yang diketahui termasuk keamanan siber dan (secara lebih umum) ketergantungan teknologi oleh negara asing. Buku Putih tahun 2008 membahas bahwa

GAMBAR 6

Hasil Polling tentang Ancaman pada Kepentingan Vital Indonesia



SUMBER: Ben Bland, Evan Laksmana, dan Natasha Kassam, “Indonesia Poll 2021: Charting Their Own Course: How Indonesians See the World,” Lowy Institute, April 2022, 13 <https://interactives.lowyinstitute.org/features/indonesia-poll-2021>

ketergantungan siber dan teknologi bisa jadi tak hanya “menjadikan Indonesia sebagai pasar belaka bagi produk asing” namun juga dapat “membuat sulit bagi Indonesia untuk mengatur ancaman-ancaman teknologi potensial yang dilakukan oleh aktor tertentu untuk memperlumah Indonesia.”¹⁰¹ Meskipun ada pengenalan bahwa ada risiko-risiko dalam ketergantungan teknologi pada negara asing, pemerintah Indonesia sudah lama menilai bahwa kemitraan internasional tambahan dan investasi asing penting bagi perkembangan Indonesia dalam bidang-bidang prioritas tinggi seperti kecerdasan buatan, cloud computing, dan 5G.¹⁰² Input-input luar negeri tersebut akan jadi aset penting Indonesia ketika negara berupaya memanen keuntungan pembangunan yang berkaitan dengan aplikasi teknologi yang cepat berubah dalam bidang seperti Internet of Things dan e-commerce.¹⁰³ Seperti dikemukakan sebelumnya, Indonesia melihat Huawei dan ZTE sebagai dua dari mitra terpentingnya dalam upaya-upaya ekonomi digital dan pembangunan.

Namun begitu, pertimbangan-pertimbangan finansial dan pembangunan hanya sebagian menjelaskan pendekatan Indonesia pada risiko keamanan yang berhubungan dengan menggunakan perusahaan-perusahaan TIK China. Risiko-risiko keamanan yang sering disebut-sebut yang dilekatkan pada infrastruktur TIK China meliputi persepsi bahwa penggunaannya dapat menaikkan bahaya dari: pencurian hak cipta intelektual, *data mining* dan surveilans, penahanan pemeliharaan dan perawatan sistem yang potensial sebagai sumber keuntungan politis, dan kemungkinan akses dan kontrol akan infrastruktur kritis (termasuk infrastruktur kesehatan masyarakat dan energi dan utilitas lain yang penting).¹⁰⁴ Namun hanya ada sedikit contoh risiko keamanan yang diketahui umum yang berasal dari penggunaan infrastruktur TIK China secara spesifik (meski banyak contoh telah timbul tentang serangan-serangan siber dari China menggunakan infrastruktur TIK negara lain). Salah satu contohnya adalah pengambilan data tanpa izin dari markas besar Uni Afrika, yang tampaknya difasilitasi oleh penggunaan software dan hardware Huawei oleh organisasi itu.¹⁰⁵ Contoh lain adalah episode yang dikemukakan dari tahun 2012 yang melibatkan Australia di mana intelijen China ternyata menginfiltrasi jajaran teknisi Huawei untuk mengkompromikan sebuah software update dari Huawei.¹⁰⁶ Walaupun hanya sedikit kejadian-kejadian terkonfirmasi mengenai risiko potensial sedemikian, keprihatinan keamanan yang disebut di muka menjadi secara teratur diungkit-ungkit dalam hubungannya dengan infrastruktur TIK China.¹⁰⁷

Tentunya, ancaman-ancaman keamanan siber yang didukung oleh pemerintah China, termasuk pencurian kekayaan intelektual dan *data mining* secara besar-besaran serta surveilans, menyebar secara global. Sebuah koalisi besar negara-negara demokrasi liberal secara bersamaan semakin mengaitkan ancaman-ancaman siber yang meluas dan kukuh ini pada pemerintah China. Penyebutan keterkaitan ini yang terbaru yang layak dicatat adalah kejadian bulan Juli 2021 yang dikaitkan dengan “aktivitas siber berbahaya dan sikap negara tak bertanggung-jawab” yang dialamatkan pada China dan Kementerian Keamanannya oleh Australia, Kanada, Uni Eropa, Jepang, Selandia Baru, Inggris, dan Amerika Serikat.¹⁰⁸ Indonesia dan negara-negara berkembang lainnya mungkin juga sudah jadi sasaran aktivitas-aktivitas siber yang luas yang didukung negara China.¹⁰⁹ Tetapi episode-episode ini belumlah dikaitkan dengan serangkaian alasan-alasan diplomatis dan politis. Yang terbaru, sebuah kelompok siber yang disponsori pemerintah China dianggap meretas server milik intelijen Indonesia.¹¹⁰ Walaupun ada ancaman-ancaman keamanan siber yang nyata dan baru yang ditimbulkan oleh aktor-aktor yang didukung pemerintah China atau aktor-aktor yang berafiliasi, tetaplah tidak jelas apakah penggunaan peralatan TIK China membuat ancaman ini lebih akut secara signifikan.¹¹¹

Pemerintah Indonesia juga menilai bahwa risiko-risiko spionase masih akan ada bila Indonesia bergantung diri pada infrastruktur yang dibangun oleh perusahaan-perusahaan Jepang, Korea Selatan, dan Eropa. Dari perspektif Amerika Serikat dan sekutu-sekutunya, keprihatinan akan

spionase yang dimungkinkan oleh siber yang berbasis negara dan ancaman-ancaman keamanan pada utamanya berpusat pada keprihatinan akan China dan Rusia, dan pada Iran serta Korea Utara pada tingkat yang lebih rendah.¹¹² Namun begitu, Indonesia juga punya keprihatinan tentang spionase Amerika Serikat dan sekutu-sekutunya serta mitra-mitranya.¹¹³ Pembocoran data oleh mantan kontraktor keamanan nasional Amerika Serikat Edward Snowden tentang spionase skala industri AS dan Australia terhadap Indonesia dan pemimpin-pemimpin politiknya bisa dipahami membuat pemerintah Indonesia melihat Amerika Serikat dan Australia sebagai sumber spionase utama dan ancaman-ancaman keamanan yang berkaitan dengannya.¹¹⁴ Sebagai contoh, bukti muncul pada bulan November 2013 mengenai kejadian Australia telah menyadap telepon anggota-anggota kunci elit politik Indonesia, termasuk presiden saat itu, Susilo Bambang Yudhoyono.

Keterlibatan yang jelas mengenai perusahaan TIK terkenal Amerika Serikat, termasuk Google dan Microsoft, dalam surveilans bersama AS dan sekutunya bisa dipahami telah menimbulkan sinisme di Indonesia berkenaan dengan klaim mengenai risiko keamanan yang meningkat berhubungan dengan perusahaan-perusahaan TIK China.¹¹⁵ Sementara itu, sebagai kontras terhadap klaim-klaim yang spekulatif kalau pemerintah China mungkin menggunakan data intelijen yang dikumpulkan lewat peralatan TIK China untuk mengecilkan keamanan ekonomi atau infrastruktur Indonesia, Australia dan Amerika Serikat mungkin sebelumnya pernah berusaha menggunakan koleksi intelijennya untuk secara ekonomi merugikan baik Indonesia maupun negara tetangganya Timor Leste.¹¹⁶ Saat infrastruktur TIK China mungkin telah membuat Indonesia rentan pada spionase berbasis siber, infrastruktur TIK Jepang, Korea Selatan, dan Eropa bukanlah hambatan bagi spionase yang berlanjut dan berat dari Amerika Serikat dan sekutunya serta mitranya. Ditambah dengan prioritas tinggi para pemimpin Indonesia pada perkembangan ekonomi dan akuisisi murah infrastruktur TIK, penilaian risiko Indonesia dari dampak vendor-vendor TIK terhadap ancaman-ancaman keamanan siber dibentuk oleh persepsi bahwa semua vendor, China atau bukan, melibatkan risiko bagi Indonesia yang susah dimitigasi.

Dunia siber menimbulkan keprihatinan baru yang berkembang untuk pemerintah Indonesia. Kesadaran keamanan siber yang rendah di antara warga mengakibatkan kurangnya penggunaan software perlindungan terhadap virus. Menurut beberapa sumber, Indonesia mengalami serangan siber sekitar 423 juta pada tahun 2020 saja.¹¹⁷ Sementara itu, sistem keamanan siber BSSN HoneyNet mencatat 246 juta serangan siber dan lebih dari 190.000 serangan malware pada tahun 2020.¹¹⁸ Indonesia juga secara teratur disebut sebagai satu di antara korban serangan siber terbesar dunia, sejumlah hampir empat per sepuluh dari “lalulintas yang berhubungan dengan peretasan global” pada tahun 2013.¹¹⁹ Serangan-serangan siber ini menyebabkan kerugian ekonomi besar. Menurut BSSN, ada 290 juta serangan siber di Indonesia pada tahun 2019, yang menyebabkan kerugian sebesar USD34,2 milyar.¹²⁰ Sebuah laporan pada tahun 2013 oleh Kominfo mengindikasikan bahwa negara ini telah

menjadi target teratas untuk serangan siber.¹²¹ Ekspansi ruang siber juga membawa pada banjirnya misinformasi dan disinformasi, dengan teori-teori konspirasi dan media *hoax* yang menodai toleransi agama dan demokrasi.¹²²

Banyak dari efek serangan-serangan siber ini di Indonesia bersifat ekonomi. Dalam satu artian, misinformasi yang disponsori negara atau serangan penolakan layanan secara terdistribusi (serangan DDoS) kurang diperhatikan daripada kejahatan siber tradisional. Tetapi hubungan antara serangan-serangan siber yang disponsori pemerintah dan kejahatan siber menjadi kabur. Pemerintah China, Rusia, Iran, dan Korea Utara juga terlibat dalam spionase ekonomi (bukan hanya spionase politis-militer) dan serangan *ransomware* untuk tujuan-tujuan ekonomi.¹²³ Sebagai contoh, serangan *ransomware* WannaCry yang diyakini dikembangkan oleh pemerintah Korea Utara, mendisrupsi layanan-layanan penting di Indonesia dan mengarah pada didirikannya badan BSSN pada tahun 2017.¹²⁴ Kementerian Keamanan China dan juga organisasi-organisasi serupa di Rusia dan Iran melibatkan kelompok-kelompok privat untuk bekerja pada mereka.¹²⁵ Staf mereka juga kadang-kadang bekerja untuk kelompok-kelompok siber privat selagi masih bekerja dalam keamanan nasional.¹²⁶ Ini membuat terbukanya kemungkinan informasi negara dengan hak istimewa dipakai untuk kejahatan siber ekonomi. Ada bukti bahwa setidaknya satu kelompok yang dikontrak oleh Kementerian Keamanan Nasional telah merekrut ahli-ahli bahasa yang fasih dalam bahasa-bahasa Asia Tenggara pula.¹²⁷

Dengan merasuknya kejahatan siber ekonomi, bahkan jika segelintir saja dari kegiatan itu adalah berkat aktor-aktor yang berkaitan dengan China, Indonesia mencari mitra untuk mendorong kemampuan keamanan sibernya. Yang patut dicatat, pemerintah China dan perusahaan-perusahaan China telah mengadaptasikan infrastruktur TIK mereka dan tawaran kerjasama teknologi yang lebih luas pada Indonesia untuk membantu mengatasi ancaman-ancaman non-negara ini.¹²⁸ Berkat kesempatan-kesempatan pelatihan dan pengembangan kapasitas dari Huawei dan ZTE yang diperingi di atas, Jakarta menilai bahwa berkolaborasi dengan infrastruktur TIK China akan membantu upayanya dalam mengatasi tantangan-tantangan berat yang utama yang ditimbulkan oleh kejahatan dan ancaman siber terhadap kohesi sosial.¹²⁹

Pemerintah China berupaya mempromosikan versi norma-norma siber dan standardnya sendiri di luar batas negaranya, termasuk Asia Tenggara. Indonesia, negara terbesar di kawasan ini, adalah target utama. Pemerintah China mempromosikan kedaulatan siber, yang merupakan versi ruang siber di mana pemerintah mengambil peran lebih mengintervensi dalam mengontrol informasi, penyimpanan data, dan akses pasar.¹³⁰ Negara-negara demokrasi liberal juga menjadi lebih mengintervensi dalam hal kebijakan internet, walau pun lebih rendah levelnya daripada di China.

Untuk mempromosikan visi ini, China telah mengadakan serangkaian dialog tentang keamanan siber di ASEAN.¹³¹ Sejumlah kecil badan pemerintah Indonesia juga telah menandatangani perjanjian siber atau MoU dengan pemerintah atau perusahaan China. Setidaknya satu badan punya referensi jelas pada tata kelola ruang siber. Sebagai contoh, sebuah MoU antara BSSN dan Cyberspace Administration of China, yang ditandatangani pada bulan Januari 2021 menyatakan bahwa “kedua belah pihak menjunjung prinsip-prinsip kedaulatan negara untuk ruang siber.”¹³² MoU juga menyebutkan bahwa kedua belah pihak akan mempromosikan “berbagi informasi sistem regulator mengenai tata kelola ruang siber yang bisa meliputi pertukaran hukum dan legislasi, kebijakan regulasi dan manajemen mengenai ruang siber.” Dokumen ini berisi bahasa yang lebih disukai Beijing tentang kedaulatan negara dan rencana untuk berbagi informasi tentang hukum. Pada tingkat ini, tak ada indikasi bahwa MoU punya efek pada tata kelola ruang siber di Indonesia. Karena penulis tak punya akses pada teks MoU dan perjanjian lain, maka detail-detail tambahan bisa saja susah didapat. Huawei dan BSSN memang menandatangani MoU tentang pengembangan kapasitas keamanan siber pada tahun 2019, yang di-upgrade menjadi persetujuan tiga pihak dengan Institut Teknologi Del pada bulan Oktober 2021.¹³³ Fokusnya pada pengembangan kapasitas keamanan siber, tapi orang bisa membayangkan perjanjian itu juga mencakup kemampuan-kemampuan legal dan legislatif seperti yang disebutkan dengan perjanjian terdahulu dengan the Cyberspace Administration of China.

Tata kelola Indonesia mengenai ruang siber berada di tengah-tengah spektrum antara praktik-praktik China dan Amerika Serikat. Indonesia punya serangkaian peraturan hukum yang kalimat-kalimatnya samar yang memungkinkan orang untuk dituntut dengan sederetan kejahatan termasuk pencemaran nama baik, “penghinaan pada agama, berkhianat, atau menggerakkan kekacauan umum.”¹³⁴ Hukum-hukum ini mempengaruhi konten online. Sebagai contoh, ada individu-individu yang dipenjarakan karena memposting secara online konten yang mendukung kemerdekaan Papua Barat, bagian timur Indonesia yang telah lama jadi rumah gerakan kemerdekaan terlarang. Di masa lampau, internet dan platform media sosial kadang-kadang ditutup atau ditunda sebagai respon terhadap gejolak di Papua Barat.¹³⁵

Juga ada legislasi baru yang berkaitan dengan siber yang sedang dibahas atau sudah menjadi kebijakan di Indonesia yang selanjutnya mereduksi kebebasan bagi para pengguna internet. Salah satu proposal yang dinamakan Peraturan Menteri No 5, yang diterbitkan oleh Menkominfo dan menjadi kebijakan pada tahun 2020, menghendaki platform apa saja yang berhubungan dengan data dari pengguna-pengguna di Indonesia untuk - menurut sebuah interpretasi - “memastikan bahwa platform mereka tidak membantu menyebarkan dokumen dan informasi terlarang - dikarakterisasikan sebagai konten yang ‘melanggar hukum Indonesia,’ mempromosikan keresahan sosial dan mengganggu aturan umum,’ atau ‘menginformasikan metode atau menyediakan akses pada informasi dan/

atau dokumen elektronik terlarang.”¹³⁶ Menkominfo punya otoritas untuk meminta konten online spesifik dihapus atau untuk mengenakan penalti jika perintah tersebut tidak diikuti dalam waktu 24 jam. (Menteri dan kementeriannya telah berganti nama beberapa kali dalam beberapa tahun lalu jadi tidak selalu diacu oleh judul yang dipakai makalah ini.) Orang awam juga bisa menyerahkan konten yang mereka yakini telah melanggar peraturan-peraturan hukum ini agar dipertimbangkan oleh pejabat-pejabat kementerian.

Logika di balik hukum ini adalah untuk memaksa perusahaan-perusahaan konten agar bertanggung-jawab terhadap informasi yang disebarkan pada platform mereka. Namun, dengan hukum Indonesia, para pemilik platform bisa saja akhirnya melakukan sensor sendiri terhadap konten yang membahas, misalnya, kemerdekaan Papua Barat, yang bisa diartikan sebagai melawan hukum Indonesia. Tetapi walaupun ada kemiripan-kemiripan antara unsur-unsur pendekatan Indonesia dan China pada tata kelola ruang siber, penulis makalah ini tak menjumpai bukti yang menyatakan bahwa hal-hal paralel itu adalah akibat pengaruh Beijing. Alih-alih, pendekatan Jakarta tampaknya didorong oleh prioritas-prioritas sosial politik dalam negeri pemerintah Indonesia. Meskipun Indonesia akan dengan senang hati menjajarkan aspek-aspek bahasa tata kelola ruang sibernya dengan China dalam MoU bersama, ini merefleksikan overlapping pandangan yang sudah ada sebelumnya dibanding hasil upaya Beijing untuk menyebarkan bahasa yang lebih disukainya.

Pelajaran Terpetik

Indonesia tak akan terbujuk untuk mengurangi ketergantungannya pada perusahaan-perusahaan TIK China dalam arti absolut, apalagi mengakhiri seluruhnya. Ini juga terjadi di negara-negara lain yang situasi pembangunannya mirip (dengan sedikit kekecualian seperti India dan Vietnam).¹³⁷ Keprihatinan yang sering disebut-sebut tentang risiko keamanan yang berkaitan dengan teknologi Huawei atau ZTE tak akan mengubah kalkulasi risiko Jakarta. Indonesia akan pertama dan utama akan melakukan akuisisi peralatan TIK dan keputusan investasi berdasar pada pertimbangan-pertimbangan pembangunan. Pemerintah-pemerintah yang berupaya mengurangi atau memoderasi peran perusahaan-perusahaan TIK China dalam pasar Indonesia yang kolosal sebaiknya membuat tawaran yang konkrit dalam pelatihan dan pengembangan kapasitas dibanding sekedar mendengarkan ancaman-ancaman keamanan atau berceramah tentang norma-norma keamanan siber.

Sebuah pendekatan yang lebih pragmatis untuk berkiprah dengan Indonesia pada isu-isu keamanan siber dan infrastruktur TIK akan lebih menguntungkan semua. Hal itu akan memberikan opsi tambahan bagi Indonesia untuk misi raksasanya dalam membangun basis infrastruktur TIK dan keahlian-keahlian digital, yang keduanya penting bagi negara ini untuk merealisasikan aspirasi

digitalnya dan ambisi-ambisi pembangunan yang lebih luas. Upaya-upaya demikian juga akan memberi Amerika Serikat dan sekutunya serta mitra-mitranya dengan jalan tambahan untuk membangun niat baik di Indonesia, seraya memastikan perusahaan-perusahaan TIK China menghadapi kompetisi yang sehat di pasar Indonesia.

Harga rendah untuk peralatan jaringan TIK akan terus menjadi poin penting, dan Indonesia akan mencari keuntungan-keuntungan tambahan dari calon-calon penyedia, seperti pelatihan dan pengembangan kapasitas. Negara-negara yang berupaya memperlambat menyebarnya perusahaan-perusahaan TIK China secara global di salah satu pasar terbesar dan ekonomi digital paling dinamis di dunia seyogyanya mempelajari contoh-contoh dari Huawei dan ZTE. Pemerintah AS seyogyanya mempertimbangkan bagaimana bila berkolaborasi dengan lembaga-lembaga pendidikan AS dan perusahaan-perusahaan TIK (atau yang dari negara sekutunya atau mitra-mitranya) untuk menyediakan Indonesia dengan skema yang menarik nilainya, termasuk infrastruktur TIK yang harganya kompetitif dan pelatihan dan pengembangan kapasitas yang relevan.

Meskipun perusahaan-perusahaan TIK China sedang membantu Indonesia membuat kemajuan untuk memenuhi harapan terbentuknya ekonomi digital dan perkembangan ekonomi yang lebih besar, tawaran-tawaran dari Huawei dan ZTE belum sepenuhnya memenuhi kebutuhan-kebutuhan infrastruktur TIK dan ahli digital di Indonesia yang masif. Untuk melengkapi tawaran dari perusahaan-perusahaan TIK China terbesar ini, Indonesia akan menyambut tawaran tambahan dalam bentuk pelatihan dan infrastruktur TIK dari Amerika Serikat dan sekutunya serta mitra-mitranya.

Tentang Penulis

Gatra Priyandita adalah analis pada International Cyber Policy Centre di Lembaga the Australian Strategic Policy Institute, di mana ia memimpin proyek riset tentang pencurian kekayaan intelektual yang dimungkinkan karena adanya siber. Ia adalah ilmuwan politik terdidik yang memiliki spesialisasi dalam kajian kebijakan luar negeri dan keamanan di Asia Tenggara. Ia memiliki gelar PhD dalam ilmu politik dari the Australian National University.

Dirk van der Kley adalah *research fellow* yang ditunjuk bersama untuk the National Security College dan the School of Regulation and Global Governance pada the Australian National University. Ia berspesialisasi dalam teori geoekonomi, sanksi-sanksi ekonomi internasional, kebijakan ekonomi internasional pemerintah China, dan efek kebijakan industri pada geopolitik.

Benjamin Herscovitch adalah *research fellow* yang ditunjuk bersama untuk the National Security College dan the School of Regulation and Global Governance pada the Australian National University. Wilayah riset utamanya adalah hubungan Australia-China, tata kelola ekonomi China, dan kebijakan luar negeri dan pertahanan Australia.

Catatan

- 1 Ben Bland, Evan Laksmana, and Natasha Kassam, “Indonesia Poll 2021: Charting Their Own Course: How Indonesians See the World,” Lowy Institute, April 2022, 13, <https://interactives.lowyinstitute.org/features/indonesia-poll-2021>.
- 2 Muhammad Zulfikar Rakhmat and Yeta Purnama, “The China Factor in Indonesia’s New Capital City Plan,” *Diplomat*, February 11, 2022, <https://thediplomat.com/2022/02/the-china-factor-in-indonesias-new-capital-city-plan>.
- 3 Penulis menanyakan setiap tokoh yang diwawancarai apakah Huawei atau ZTE punya reputasi buruk. Setiap orang dari mereka menjawab bahwa tak satupun dari kedua perusahaan itu punya citra negatif. Tentunya, para individu ini bersikap kritis akan ketergantungan pada teknologi China. Namun hanya sangat sedikit contoh, walaupun ada, tentang populernya protes terhadap Huawei atau ZTE dan sangat sedikit contoh yang berkenaan dengan isu pemilu. Protes pada jenis lain investasi perusahaan China adalah umum. Sebagai contoh lihat Amy Chew, “Indonesian Students in Sulawesi Continue Protests Against Chinese Workers,” *South China Morning Post*, July 16, 2020, <https://www.scmp.com/week-asia/politics/article/3093345/indonesian-students-sulawesi-continue-protests-against-chinese>.
- 4 Wawancara penulis dengan seorang pejabat senior pemerintah Indonesia dilakukan pada bulan Februari 2022.
- 5 Chuin-Wei Yap, “State Support Helped Fuel Huawei’s Global Rise,” *Wall Street Journal*, December 27, 2019, <https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736>.
- 6 Poin ini dibuat oleh hampir semua tokoh yang diwawancarai tanpa memandang bagaimana keterlibatan Huawei dan ZTE dalam infrastruktur digital Indonesia. Wawancara penulis dengan sejumlah pejabat senior, akademisi, dan nara sumber kalangan industri Indonesia, Desember 2021 sampai Maret 2022.
- 7 Yohana Arthur Uly, “Garap Pasar 5G Indonesia, Ini Strategi Huawei,” [Working on the Indonesian 5G Market, This is Huawei’s Strategy], *Kompas*, January 15, 2021, <https://money.kompas.com/read/2021/01/15/121300626/garap-pasar-5g-indonesia-ini-strategi-huawei?page=all>.
- 8 Sebagai contoh, laporan tahunan Huawei pada 2021 menyatakan, “Di Indonesia, kami memperbarui Memorandum of Understanding (MoU) pada kerja sama keamanan siber dengan Badan Siber dan Sandi Negara (BSSN), meyakinkan kembali komitmen kami untuk saling berbagi pengetahuan keamanan siber dan mendukung rencana Indonesia untuk mengembangkan profesional-profesional keamanan siber dan transformasi digital.” Lihat Huawei Investment and Holding Company, “Huawei Annual Report,” Huawei Investment and Holding Company, 85, https://web.archive.org/web/20220403102653/https://www-file.huawei.com/minisite/media/annual_report/annual_report_2021_en.pdf.
- 9 Kiki Siregar, “Spate of Cyberattacks in Indonesia Shines Spotlight on Complacency, Public Education,” *Channel News Asia*, December 18, 2021, <https://www.channelnewsasia.com/asia/indonesia-cyberattacks-complacency-education-bssn-bnpb-2386586>.
- 10 Wawancara penulis dengan spesialis keamanan siber pada bulan Februari 2022.
- 11 Wawancara penulis dengan pejabat pemerintah Indonesia, December 2021 to March 2022.
- 12 Ini dihitung dari data World Bank. Menurut data tersebut, pada 2020 PDB per kapita Amerika Serikat (dalam USD sekarang) \$63.593, dan PDB per kapita Indonesia \$3.870. Pada 1991, Amerika Serikat memiliki PDB per kapita \$24.342 dan Indonesia memiliki PDB per kapita \$632. Lihat World Bank, “World Development Indicators,” World Bank, 2020, <https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=US-ID-KR>.
- 13 Bain and Company, “Technology Report 2021: The ‘20s Roar,” Bain and Company, 2021, 3, https://www.bain.com/globalassets/noindex/2021/bain_report_technology-report-2021.pdf.
- 14 Sanya DS, Fardah, “Digital Technology Has Potential to Create 20–45 Million New Jobs,” *Antara News*, February 21, 2022, <https://web.archive.org/web/20220317093045/https://en.antaranews.com/news>

- [/216457/digital-technology-has-potential-to-create-20-45-million-new-jobs](#); and Indonesian Investment Coordinating Board, “Making Indonesia 4.0: Indonesia’s Strategy to Enter the 4th Generation of Industry Revolution,” Indonesian Investment Coordinating Board, April 27, 2018, <https://web.archive.org/web/20220217114250/https://www9.investindonesia.go.id/en/why-invest/indonesia-economic-update/making-indonesia-4.0-indonesias-strategy-to-enter-the-4th-generation-of-ind>.
- 15 The International Trade Administration, “Indonesia: Digital Economy Opportunities,” U.S. Department of Commerce, December 9, 2021, <https://www.trade.gov/market-intelligence/indonesia-digital-economy-opportunities>.
 - 16 Indonesian Ministry of Communication and Informatics, “National E-Government Road Map 2016–2019,” Indonesian Ministry of Communication and Informatics, January 21, 2016, https://web.archive.org/web/20220622152138/https://kominfo.go.id/content/detail/6620/siaran-pers-nollpihkom/infol2016-tentang-pemerintah-selesaikan-petajalan-iegovernmenti-2016-2019-yang-bernuansa-nawacita-dengan-menyerapinisiatif-dari-semua-kementerian-dan-lembaga-terkait/0/siaran_pers.
 - 17 Medha Basu, “Indonesia Reveals Digital Economy Targets,” GovInsider, April 21, 2017, <https://govinsider.asia/innovation/indonesia-reveals-digital-economy-targets>.
 - 18 Indonesian Investment Coordinating Board, “Making Indonesia 4.0.”
 - 19 Anthony Iswara, “Indonesia Sets Sights on Artificial Intelligence in New National Strategy,” *Jakarta Post*, August 14, 2020, <https://www.thejakartapost.com/news/2020/08/13/indonesia-sets-sights-on-artificial-intelligence-in-new-national-strategy.html>.
 - 20 Arindra Meodia, “Ministry Drafts Roadmap for Indonesia Digital 2021–2024,” *Antara News*, February 1, 2021, <https://en.antaranews.com/news/167151/ministry-drafts-roadmap-for-indonesia-digital-2021-2024>; and Lifa Putri and Fadhli Ruhman, “Minister Outlines Priorities Within Digital Indonesia Road Map,” *Antara News*, March 23, 2022, <https://en.antaranews.com/news/221329/minister-outlines-priorities-within-digital-indonesia-road-map>.
 - 21 World Bank, “Preparing ICT Skills for Digital Economy: Indonesia Within the ASEAN Context,” World Bank, March 8, 2018, https://blogs.worldbank.org/sites/default/files/preparing_ict_skills_for_digital_economy-revised_7mar2018.pdf.
 - 22 World Bank, “Population, Total – Indonesia,” World Bank, 2020, <https://data.worldbank.org/indicator/SP.POPTOTL?locations=ID>.
 - 23 Eisy A. Eloksari, “Indonesian Internet Users Hit 196 Million, Still Concentrated in Java: APKII Survey,” *Jakarta Post*, November 11, 2020, <https://www.thejakartapost.com/news/2020/11/11/indonesian-internet-users-hit-196-million-still-concentrated-in-java-apkii-survey.html>
 - 24 Darlena Cunha, “The Common Room: How an Artist Is Connecting Rural Indonesia One Village at a Time,” Internet Society, April 28, 2021, <https://www.internetsociety.org/blog/2021/04/the-common-room-how-an-artist-is-connecting-rural-indonesia-one-village-at-a-time>; dan wawancara penulis dengan spesialis keamanan siber Indonesia, Januari 2022.
 - 25 Wawancara penulis dengan sejumlah pejabat senior Indonesia, akademisi, dan nara sumber kalangan industri, Desember 2021 - Maret 2022.
 - 26 Onno W. Purbo, “Narrowing the Digital Divide,” in *Digital Indonesia: Connectivity and Divergence*, edited by Edwin Jurriens and Ross Tapsell (Singapore: ISEAS, 2017): 75–92; and Indonesian Embassy in the United States, “Facts and Figures,” Indonesian Embassy in the United States, <https://web.archive.org/web/20220619160848/https://www.embassyofindonesia.org/basic-facts/>.
 - 27 Eloksari, “Indonesian Internet Users Hit 196 Million, Still Concentrated in Java.”
 - 28 Aadarsh Baijal, Alessandro Cannarsi, and Florian Hoppe, “e-Conomy SEA 2020,” Google, Temasek, and Bain and Company, November 10, 2020, 96, <https://www.bain.com/insights/e-conomy-sea-2020>.
 - 29 Ibid.

- 30 Ibid., 32.
- 31 “Indonesia’s Digital Economy to Reach \$146 Billion in 2025: President,” *Antara News*, December 15, 2021, <https://en.antaraneews.com/news/204589/indonesias-digital-economy-to-reach-146-billion-in2025-president>
- 32 United Nations Department of Economic and Social Affairs, Population Division, “Indonesia,” in *World Population Prospects 2019, Volume II: Demographic Profiles*, 2019, https://population.un.org/wpp/Graphs/1_Demographic%20Profiles/Indonesia.pdf.
- 33 Statista, “Number of Social Network Users in Selected Countries in 2021 and 2026,” July 2021, <https://www.statista.com/statistics/278341/number-of-social-network-users-in-selectedcountries/#:~:text=China%20is%20the%20biggest%20social,million%20current%20social%20media%20users.>
- 34 Petir Garda Bhwana, “SOEs Minister Says Expect Number of Unicorns to Increase,” *Tempo*, January 16, 2022, <https://en.tempo.co/read/1550480/soes-minister-says-expect-number-of-unicorns-to-increase>.
- 35 Joko Widodo, “Remarks of President of the Republic of Indonesia in Virtual ASEAN Business and Investment Summit,” Presidential Palace, October 25, 2021, <https://web.archive.org/web/20220622152732/https://setkab.go.id/en/remarks-of-president-of-the-republic-of-indonesia-in-virtual-asean-business-and-investment-summit-25-october-2021-at-bogor-presidential-palace-west-java-province/>.
- 36 Kayla Goode and Heeu Millie Kim, “Indonesia’s AI Promise in Perspective,” Georgetown University Center for Security and Emerging Technology, 2021, 20, <https://doi.org/10.51593/2021CA001>.
- 37 Henry Tugendhat, “How Huawei Succeeds in Africa: Training and Knowledge Transfers in Kenya and Nigeria,” Johns Hopkins University School of Advanced International Studies, China Africa Research Initiative, Working Paper No. 2020/34, <https://www.econstor.eu/bitstream/10419/248162/1/sais-cari-wp34.pdf>.
- 38 Ibid.
- 39 Stefan Pongratz, “Key Takeaways – 2021 Total Telecom Equipment Market,” Dell’Oro Group, March 14, 2022, <https://www.delloro.com/key-takeaways-2021-total-telecom-equipment-market>.
- 40 Wawancara penulis dengan sejumlah pejabat senior Indonesia, akademisi, dan kalangan industri, Desember 2021 sampai Maret 2022.
- 41 Laporan riset privat yang dibeli penulis dari 6WResearch
- 42 Korespondensi penulis lewat email dengan personalia Huawei, Juli 2022.
- 43 Uday Rayana, “Sejarah ZTE di Indonesia, Kerjasama dengan Smartfren Menjadi Titik Balik Pertumbuhan,” [History of ZTE in Indonesia, Cooperation With Smartfren Turning Point for Growth], *Selular*, April 20, 2022, <https://selular.id/2022/04/sejarah-zte-di-indonesia-kerjasama-dengan-smartfren-menjadi-titik-balik-pertumbuhan>.
- 44 Chinese Ministry of Foreign Affairs, “Ambassador Xiao Qian Visits Huawei Indonesia,” May 28, 2018, <https://web.archive.org/web/20220622151112/https://www.fmprc.gov.cn/ce/ceindo/eng/sgdt/t1562928.htm>.
- 45 Koesmarihati Sugondo and Risa Bhinekawati, “Indonesia: Telecommunications on a Road to Reforms,” in *Telecommunications Reform in the Asia-Pacific Region*, edited by Allan Brown, Moazzem Hossain, and Duc-Tho Nguyen (Cheltenham, UK: Edward Elger, 2004), 102.
- 46 Ahmad Budi Setiawan, Onny Rafizan, and Ashwin Sasongko Sastrosubroto, “Development of the Information and Communication Technology Service Industry in Indonesia,” *Journal of Telecommunications and the Digital Economy* 5, no. 3 (2017): 56–60.
- 47 Merlyna Lim, “The Internet, Social Networks, and Reform in Indonesia,” in *Contesting Media Power: Alternative Media in a Networked World*, edited by Nick Couldry and James Curran (Oxford: Rowman and Littlefield Publishers, 2003), 276.
- 48 “Huawei Wins Contract from Indonesia,” *SinoCast China IT Watch*, (found on Factiva), June 23, 2003.

- 49 Jessica Ramakrishnan, "ZTE Wins CDMA 1X Contract From Indosat," *IHS Markit*, (found on Factiva), February 16, 2004
- 50 "Telkom Awards Turnkey Cable Contract to Huawei Subsidiary," Comms Update, December 15, 2009, <https://www.commsupdate.com/articles/2009/12/15/telkom-awards-turnkey-cable-contract-to-huawei-subsidiary>; "Huawei Marine Upgrades PT Telkom 3rd Route Submarine Cable," *Offshore Energy*, March 27, 2014, <https://www.offshore-energy.biz/huawei-marine-upgrades-pt-telkom-3rd-route-submarine-cable>; and "Serat Optik Mataram-Kupang Beroperasi April 2011," [Mataram-Kupang Optical Fiber to be Operational in April 2011], *Kompas*, March 1, 2011, <https://money.kompas.com/read/2011/03/01/22130497/index-html>.
- 51 "Uji Coba Jaringan LTE, ZTE Jalin Kerjasama dengan Telkomsel" [LTE Network Trial, ZTE Cooperates With Telkomsel], *Tempo*, September 21, 2010, <https://tekno.tempo.co/read/279413/uji-coba-jaringan-lte-zte-jalin-kerjasama-dengan-telkomsel>; "Smartfren Launches LTE-A in Jakarta," Comms Update, August 21, 2015, <https://www.commsupdate.com/articles/2015/08/21/smartfren-launches-lte-a-in-jakarta> and "Smartfren 4G LTE Rollout Reaches 85 Cities," Comms Update, January 27, 2016, <https://www.commsupdate.com/articles/2016/01/27/smartfren-4g-lte-rollout-reaches-85-cities>.
- 52 "ZTE Supported Makassar Smart City Solution," IndoTelko.com, August 19, 2015, accessed 15 May 2022, <https://www.indotelko.com/read/1439949857/zte-makassar-smart-city-solution>.
- 53 Rhenald Kasali, *Cracking Zone* (Jakarta: PT Gramedia, 2010), 50.
- 54 Wawancara penulis dengan pejabat-pejabat pemerintah dan spesialis keamanan siber, Desember 2021 sampai Maret 2022.
- 55 Ali Farhoomand and Phoebe Ho, "Huawei: Cisco's Chinese Challenger," University of Hong Kong, 2006, <https://hbsp.harvard.edu/product/HKU599-PDF-ENG>.
- 56 Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 27, 2019, <https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736>; and Alan Weissberger, "WSJ: China's Financial Support Aided Huawei's Rise to #1 Telecom Vendor in the World," IEEE Communications Society Technology Blog, December 26, 2019, <https://techblog.comsoc.org/2019/12/26/wsj-chinas-financial-support-aided-huaweis-rise-to-1-telecom-vendor-in-the-world>.
- 57 Ibid.
- 58 "Chinese Government Pledges to Extend 200 Million USD Export Credit to Indonesia," AidData, <https://china.aiddata.org/projects/38656/>; "Chinese Government Pledges to Provide \$300 Million Preferential Buyer's Credit Loan for Earthquake Reconstruction Activities," AidData, <https://china.aiddata.org/projects/35147/>; and Sumner Lemon, "China to Finance \$1.1B in Telecom Equipment Exports," *InfoWorld.com*, February 20, 2004, <https://www.infoworld.com/article/2667946/china-to-finance--1-1b-in-telecom-equipment-exports.html>.
- 59 Industrial and Commercial Bank of China, "The World's First Renminbi Export Buyer's Credit Business Settled in ICBC," Industrial and Commercial Bank of China, August 18, 2010, <https://web.archive.org/web/20220622171922/http://www.icbc-ltd.com/icbc/en/newsupdates/icbc%20news/The%20Worlds%20First%20Renminbi%20Export%20Buyers%20Credit%20Business%20Settled%20in%20ICBC.htm>.
- 60 "CDB Provides \$29.75 Million Buyer's Credit Loan for ZTE Fiber-to-the-Home (FTTH) Network Project," AidData, <https://china.aiddata.org/projects/66446>.
- 61 "Huawei Wins Contract From Indonesia," *SinoCast China IT Watch*, (found on Factiva), June 23, 2003
- 62 "ZTE Opens Telecoms Training Centre in Indonesia," *DMAAsia*, (found on Factiva), May 8, 2006
- 63 Yudha Pratomo, "BSSN dan Huawei Kerja Sama Kembangkan SDM untuk Keamanan Siber," [BSSN and Huawei Cooperate to Develop Human Resources for Cybersecurity], *Kompas*, October 29, 2019,

- <https://tekno.kompas.com/read/2019/10/29/15460047/bssn-dan-huawei-kerja-sama-kembangkan-sdm-untuk-keamanan-siber>; and Yuni Arisandy Sinaga, “Huawei Strengthens Cyber Security Cooperation With Indonesia,” *Antara News*, September 28, 2021, <https://web.archive.org/web/20220211113933/https://en.antaranews.com/news/191381/huawei-strengthens-cyber-security-cooperation-with-indonesia>.
- 64 Koya Jibiki and Takashi Kawakami, “Huawei’s 5G Deal With Indonesia Spearheads Southeast Asia Push,” *Nikkei Asia*, December 2, 2020, <https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-s-5G-deal-with-Indonesia-spearheads-Southeast-Asia-push>; and “ZTE and Telkomsel Present 5G Use Cases at Telkomsel 5G Launch Event,” *Jakarta Globe*, July 2, 2021, <https://jakartaglobe.id/tech/zte-and-telkomsel-present-5g-use-cases-at-telkomsel-5g-launch-event/>.
- 65 Australian Trade and Investment Commission, “Digital Technology to Indonesia: Trends and Opportunities,” Australian Trade and Investment Commission, <https://www.austrade.gov.au/australian/export/export-markets/countries/indonesia/industries>.
- 66 Ibid.
- 67 Uly, “Garap Pasar 5G Indonesia, Ini Strategi Huawei,” [Working on the Indonesian 5G Market, This is Huawei’s Strategy].
- 68 “Program Huawei Seeds for the Future Ajak Mahasiswa Terbaik Indonesia Belajar Inovasi Teknologi di Tiongkok,” [Huawei Seeds for the Future Program Invites the Best Indonesian Students to Study Technological Innovation in China], *Daily Social Newswire*, December 10, 2015, <https://dailysocial.id/wire/program-huawei-seeds-for-the-future-ajak-mahasiswa-terbaik-indonesia-belajar-inovasi-teknologi-di-tiongkok>.
- 69 “Huawei Seeds for the Future 2021 Readies Digital Talents for Future of Work,” *Jakarta Globe*, November 2021, <https://jakartaglobe.id/special-updates/huawei-seeds-for-the-future-2021-readies-digital-talents-for-future-of-work/#:~:text=Jakarta,.in%20Indonesia%20and%20the%20world>.
- 70 Ratri Adityarani, “China’s Huawei Opens Technology Training Center in Indonesia,” *Tech in Asia*, April 12, 2011, <https://www.techinasia.com/china-huawei-opens-technology-training-center-in-indonesia>.
- 71 “Huawei Brings Digital Economy-Based Training and Wealth to State Colleges,” *China Daily*, May 15, 2017, https://web.archive.org/web/20200417065638/https://www.chinadaily.com.cn/cndy/2017-05/15/content_29345046.htm.
- 72 “BSSN dan Huawei Kerja Sama Kembangkan SDM untuk Keamanan Siber,” [BSSN and Huawei Cooperate to Develop Human Resources for Cyber Security], *Kompas*, October 29, 2019, <https://tekno.kompas.com/read/2019/10/29/15460047/bssn-dan-huawei-kerja-sama-kembangkan-sdm-untuk-keamanan-siber>.
- 73 “Huawei Strengthens Contribution and Cooperation in Indonesia Cyber Security,” Huawei, September 28, 2021, <https://web.archive.org/web/20211004105819/https://www.huawei.com/en/news/2021/9/tripartite-cooperation-agreement-indonesia-cyber-security>.
- 74 Uly, “Garap Pasar 5G Indonesia, Ini Strategi Huawei,” [Working on the Indonesian 5G Market, This is Huawei’s Strategy].
- 75 Jayanty Nada Shofa, “Huawei Affirms Support for Indonesia’s Digital Transformation With New Academy,” *Jakarta Globe*, January 26, 2021, <https://jakartaglobe.id/tech/huawei-affirms-support-for-indonesias-digital-transformation-with-new-academy>.
- 76 “Dukung Pengembangan Teknologi Tanah Air, ZTE Dirikan Public Training Center di Indonesia,” [Supporting National Technology Development, ZTE Establishes Public Training Center in Indonesia], *Kompas*, June 24, 2021, <https://biz.kompas.com/read/2021/06/24/142410328/dukung-pengembangan-teknologi-tanah-air-zte-dirikan-public-training-center-di>.

- 77 ZTE, “ZTE Opens Telecoms Training Centre in Indonesia,” ZTE, June 19, 2006, https://web.archive.org/web/20220622154724/https://www.zte.com.cn/global/about/magazine/zte-technologies/2006/6/en_156/161603.html.
- 78 Gayatri Suroyo, “Alibaba’s Jack Ma Says in Talks With Indonesia on Tech Training Institute,” Reuters, October 13, 2018, <https://www.reuters.com/article/us-imf-worldbank-tech-alibaba/alibabas-jack-ma-to-open-institute-for-tech-entrepreneurs-in-indonesia-idUSKCN1MN08U>.
- 79 Huawei, “Huawei Strengthens Contribution and Cooperation in Indonesia’s Cybersecurity.”
- 80 Binus University and Apple offer a free joint ten-month developer program designed to get developers working on apps in Apple’s ecosystem. See “Frequently Asked Questions,” Binus Development Academy, May 24, 2022, <https://web.archive.org/web/20220622175740/https://developeracademy.apps.binus.ac.id/faq/>.
- 81 Brandon Vigliarolo, “The Apple Developer Program: What Professionals Need to Know,” Tech Republic, Juni 4, 2021, <https://www.techrepublic.com/article/the-apple-developer-program-what-professionals-need-to-know/#:~:text=This%20is%20the%20unfortunate%20part,the%20form%20of%20app%20> dan wawancara penulis dengan Onno W. Purbo, Februari 2022
- 82 Wawancara penulis dengan Onno W. Purbo, Februari 2022.
- 83 Wawancara penulis dengan Onno W. Purbo, Februari 2022.
- 84 “Huawei Strengthens Contribution and Cooperation in Indonesia’s Cybersecurity,” *Jakarta Globe*.
- 85 Wawancara penulis dengan sejumlah pejabat senior Indonesia, akademisi, dan narasumber kalangan industri, Desember 2021 sampai Maret 2022.
- 86 Wawancara penulis dengan sejumlah pejabat senior Indonesia, akademisi, dan narasumber kalangan industri, Desember 2021 sampai Maret 2022.
- 87 Wawancara penulis dengan Onno W. Purbo, Februari 2022.
- 88 Tugendhat, “How Huawei Succeeds in Africa: Training and Knowledge Transfers in Kenya and Nigeria.”
- 89 Chinese Ministry of Foreign Affairs, “China-ASEAN Cooperation in 2012,” Chinese Ministry of Foreign Affairs, November 19, 2012, <https://web.archive.org/web/20220622173218/https://www.mfa.gov.cn/ce/cela/eng/news/t990470.htm>.
- 90 Niva Yau and Dirk van der Kley, “China’s Global Network of Vocational Colleges to Train the World,” *Diplomat*, November 11, 2021, <https://thediplomat.com/2021/11/chinas-global-network-of-vocational-colleges-to-train-the-world>.
- 91 Yau and van der Kley, “China’s Global Network of Vocational Colleges to Train the World”; Chinese Ministry of Education, “Luban Workshop—China’s Vocational Education Going Global,” *China Education Daily* (published on the ministry’s website), May 11, 2018, https://web.archive.org/web/20220622173342/http://en.moe.gov.cn/Specials/Specials_40th/Achievements/201805/t20180531_337956.html.
- 92 Yau and van der Kley, “China’s Global Network of Vocational Colleges to Train the World.”
- 93 Chinese Ministry of Education, “Luban Workshop—China’s Vocational Education Going Global.”
- 94 “China Sets Up Tech Transfer Centers With ASEAN Countries,” State Council, June 17, 2015, https://web.archive.org/web/20220622173621/http://english.www.gov.cn/news/top_news/2015/06/17/content_281475129044252.htm.
- 95 Xiaolin Zhou, “Case Study From China: CATTC - China-ASEAN Technology Transfer Center,” Organisation for Economic Co-operation and Development’s TIP Co-Creation Project, December 9, 2020, 1, <https://stip.oecd.org/assets/TKKT/CaseStudies/38.pdf>.
- 96 “Zhongguo: Dongmeng Wangluo Anquan Jiaoliu Peixun Zhongxin Zhengshi Jiepai,” [China-ASEAN Cybersecurity Exchange and Training Center Officially Opens], Sohu, October 29, 2019, https://web.archive.org/web/20220622173922/https://www.sohu.com/a/350380499_114731.

- 97 Sebagai contoh, pemerintah Swiss telah berinvestasi dalam pelatihan keahlian di Indonesia. Lihat P. John Williams dan Shaun Wellbourne-Wood, “Opportunities for Western Australian VET Providers in East Java,” Western Australian Department of Jobs, Tourism, Science, and Innovation and Austrade, February 4, 2022, 45, <https://www.wa.gov.au/system/files/2021-01/Opportunities%20for%20WA%20VET%20providers%20in%20East%20Java.pdf>.
- 98 Lihat bab “Security and Threats” dalam publikasi berikut. Bland, Laksmana, and Kassam, “Indonesia Poll 2021: Charting Their Own Course.”
- 99 *Rencana Kerja Pertahanan Negara Tahun 2013* [National Defence Strategic Plan, 2013] (Jakarta: Ministry of Defence, 2013), 12.
- 100 Buku Putih Pertahanan Indonesia 2008 [2008 Indonesian Defence White Paper] (Jakarta: Ministry of Defence, 2008) <https://web.archive.org/web/20220622174232/https://www.kemhan.go.id/ppid/wp-content/uploads/sites/3/2015/12/04f92fd80ee3d01c8e5c5dc3f56b34e3.pdf> and “Spotlight on Indonesia: Seizing the Digital Transition Opportunity Now,” GSMA, <https://www.gsma.com/spectrum/wp-content/uploads/2020/02/Indonesia-Digital-Dividend.pdf>.
- 101 Buku Putih Pertahanan Indonesia 2008 [2008 Indonesian Defence White Paper], 38.
- 102 Goode and Kim, *Indonesia’s AI Promise in Perspective*, 20.
- 103 “China-Indonesia Technology Transfer Center,” Chinese Embassy in Indonesia, April 22, 2014, <https://web.archive.org/web/20220622174500/https://www.fmprc.gov.cn/ce/ceindo/eng/whjy/kjil/t1149138.htm>.
- 104 Danielle Cave, Elsa Kania, Tom Uren, Fergus Hanson, Peter Jennings, Michael Shoebridge, Samantha Hoffman, Jessica Clarence and Greg Austin, “Huawei and Australia’s 5G Network,” Australian Strategic Policy Institute, 2018, <https://www.aspi.org.au/report/huawei-and-australias-5g-network>.
- 105 Danielle Cave, “The African Union Headquarters Hack and Australia’s 5G Network,” *Strategist*, July 13, 2018, <https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network>.
- 106 Jordan Robertson and Jamie Tarabay, “Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack,” Bloomberg, December 17, 2021, <https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack> and Jordan Robertson and Jamie Tarabay, “Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack,” BNN Bloomberg, December 16, 2021, <http://origin.bnn.ca/chinese-spies-accused-of-using-huawei-in-secret-australia-telecom-hack-1.1697167>.
- 107 Peter Hartcher, “Huawei? No Way! Why Australia Banned the World’s Biggest Telecoms Firm,” *Sydney Morning Herald*, May 21, 2021, <https://www.smh.com.au/national/huawei-no-way-why-australia-banned-the-world-s-biggest-telecoms-firm-20210503-p57oc9.html>.
- 108 White House, “The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China,” White House, July 19, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china>; and Steve Holland and Doina Chiacu, “U.S. and Allies Accuse China of Global Hacking Spree,” Reuters, July 20, 2021, <https://www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19/>.
- 109 Sejumlah pejabat senior pemerintah Indonesia dan pakar-pakar keamanan siber yang diwawancarai mencatat bahwa badan intelijen China mungkin bertanggung jawab pada beberapa serangan siber yang belum diumumkan kaitannya secara publik. Wawancara penulis dengan beberapa pejabat Indonesia dan pakar keamanan siber, Desember 2021 sampai Maret 2022.
- 110 Resty Woro Yuniar, “Indonesia Denies Report of Chinese Hacking Group Breaching Intelligence Agency Servers,” *South China Morning Post*, September 14, 2021, <https://www.scmp.com/week-asia/politics/article/3148680/indonesia-denies-report-chinese-hacking-group-breaching>.

- 111 Sejumlah pejabat pemerintah Indonesia dan pakar-pakar keamanan siber yang diwawancarai untuk makalah ini mencatat besarnya ancaman keamanan siber dari China tapi tak yakin apakah penggunaan peralatan Huawei and ZTE akan sangat memperburuk ancaman ini. Wawancara penulis dengan sejumlah pejabat Indonesia dan pakar-pakar keamanan siber. Desember 2021 sampai Maret 2022.
- 112 See, for example, *ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021* (Australia Cyber Security Centre, Canberra: 2021), <https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf>.
- 113 Evan A. Laksmana, "Pragmatic Equidistance: How Indonesia Manages Its Great Power Relations," in *China, the United States, and the Future of Southeast Asia*, edited by David Denoon (New York: New York University Press, 2017), 113–135, <https://ssrn.com/abstract=2761998>.
- 114 Philip Dorling, "Edward Snowden Leak: Australia Spied on Indonesian Phones and Data," *Sydney Morning Herald*, February 17, 2014, <https://www.smh.com.au/politics/federal/edward-snowden-leak-australia-spied-on-indonesian-phones-and-data-20140216-32tux.html>; and Ewen MacAskill and Lenore Taylor, "Australia's Spy Agencies Targeted Indonesian President's Mobile Phone," *Guardian*, November 18, 2013, <https://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone>.
- 115 Ewen MacAskill, "NSA Paid Millions to Cover Prism Compliance Costs for Tech Companies," *Guardian*, August 24, 2013, <https://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid>.
- 116 Christopher Knaus, "Witness K and Lawyer Bernard Collaery Helped Correct What They Saw as a Gross Injustice. They Now Face Jail Time," *Guardian*, August 10, 2019, <https://www.theguardian.com/australia-news/2019/aug/10/witness-k-and-the-outrageous-spy-scandal-that-failed-to-shame-australia>; and "NSA Australia Allies 'Spied on US Law Firm' in Indonesia Row," *BBC News*, February 16, 2014, <https://www.bbc.com/news/world-us-canada-26216883>.
- 117 Greta Nabbs-Keller and RM Wibawanto Nugroho Widodo, "Indonesia Responds to the Cyber Dark Side," Lowy Institute's *Interpreter*, May 13, 2021, <https://www.lowyinstitute.org/the-interpreter/indonesia-responds-cyber-dark-side>.
- 118 Jayanty Nada Shofa, "Huawei Affirms Support for Indonesia's Digital Transformation With New Academy," *Jakarta Globe*, January 26, 2021, <https://jakartaglobe.id/tech/huawei-affirms-support-for-indonesias-digital-transformation-with-new-academy/>.
- 119 "Indonesia Overtakes China as Top Source of Cyber Attack Traffic," *ABC*, October 18, 2013, <https://www.abc.net.au/news/2013-10-18/an-indonesia-overtakes-china-as-top-source-of-cyber-attack-traf/5032428>.
- 120 Hoor Halimah Anjani, "Policy Brief: Cybersecurity Protection in Indonesia," Center for Indonesian Policy Studies, Policy Brief No. 9, July 11, 2011, <https://www.econstor.eu/bitstream/10419/249442/1/CIPS-PB09.pdf>.
- 121 "Indonesia World's No. 1 Target for Cyber Attacks," *Asmag*, December 31, 2013, <https://www.asmag.com/showpost/28975.aspx>.
- 122 Thomas Paterson, "Indonesian Cyberspace Expansion: A Double-Edged Sword," *Journal of Cyber Policy* 4, no. 2 (2019): 216–234.
- 123 Adam Segal, Samantha Hoffman, Fergus Hanson, and Tom Uren, "Hacking for Ca\$h," Australian Strategic Policy Institute, September 25, 2018, <https://www.aspi.org.au/report/hacking-cash>.
- 124 Fransiska Nangoy and Agustinus Da Costa, "Two Major Indonesian Hospitals Attacked in 'Ransomware' Storm," Reuters, May 13, 2017, <https://www.reuters.com/article/us-cyber-attack-indonesia-idUSKBN1890AX>.

- 125 Paul Mozur and Chris Buckley, “Spies for Hire: China’s New Breed of Hackers Blends Espionage and Entrepreneurship,” *New York Times*, August 26, 2021, <https://www.nytimes.com/2021/08/26/technology/china-hackers.html>.
- 126 Ibid.
- 127 Ibid.
- 128 Menurut pernyataan pengakuan dari Amerika Serikat dan sejumlah sekutu dan mitranya, beberapa spionase China yang berbasis negara telah dilakukan dalam kolaborasi dengan penjahat-penjahat kriminal siber. Lihat Kementerian Luar Negeri Australia, “Australia Joins International Partners in Attribution of Malicious Cyber Activity to China,” Kementerian Luar Negeri Australia, Juli 19, 2021, <https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china>. Jakarta mungkin masih menganggap bahwa ancaman utama yang dihadapinya adalah dari tindak kriminal siber dibanding spionase berbasis negara dan ancaman keamanan. Jakarta bisa jadi juga percaya bahwa China tak akan menggunakan taktik demikian terhadap Indonesia.
- 129 Huawei, “Huawei Strengthens Contribution and Cooperation in Indonesia Cyber Security.”
- 130 Adam Segal, “China’s Vision for Cyber Sovereignty and the Global Governance of Cyberspace,” National Bureau of Asian Research Special Report no. 87, August 25, 2020, <https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/>.
- 131 Tentang Kerjasama tata kelola siber China-ASEAN, lihat, sebagai contoh, Kementerian Luar Negeri China, “Co-Chairs’ Statement on the 1st ASEAN-China Cyber Dialogue,” Kementerian Luar Negeri China, Desember 16, 2020, https://web.archive.org/web/20220622174812/https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202012/t20201216_599781.html; ASEAN-China Centre, “The China-ASEAN Information Harbor Digital Silk Road Industry Cooperation Forum Successfully Held,” ASEAN-China Centre, November 25, 2020, <https://web.archive.org/web/20220622174930/http://www.asean-china-center.org/english/2020-11/5581.html>; and General Office of Hubei Provincial People’s Government, “China-ASEAN Digital Economy Development and Cooperation Forum to Be Held in Wuhan,” General Office of Hubei Provincial People’s Government, July 14, 2021, https://web.archive.org/web/20220622175454/http://en.hubei.gov.cn/news/newslst/202107/t20210714_3644952.shtml.
- 132 “Memorandum of Understanding antara BSSN Republik Indonesia dan the Cyberspace Administration of the People’s Republic of China mengenai Kerjasama dalam Mengembangkan Kapasitas Keamanan Siber dan Teknologi.” Penulis memiliki akses privat ke dokumen ini.
- 133 Huawei, “Huawei Strengthens Contribution and Cooperation in Indonesia Cyber Security.”
- 134 Eduard Lazarus, “The Authoritarian Threat of Indonesia’s Latest Internet Bill,” Lowy Institute’s *Interpreter*, June 7, 2021, <https://www.lowyinstitute.org/the-interpreter/authoritarian-threat-indonesia-s-latest-internet-bill>.
- 135 “Indonesia,” Freedom House Index, 2019, <https://freedomhouse.org/country/indonesia/freedom-net/2019>.
- 136 Eduard Lazarus, “The Authoritarian Threat of Indonesia’s Latest Internet Bill,” Lowy Institute’s *Interpreter*, June 7, 2021, <https://www.lowyinstitute.org/the-interpreter/authoritarian-threat-indonesia-s-latest-internet-bill>.
- 137 “Vietnam Shuns Huawei as It Seeks to Build Southeast Asia’s First 5G Network,” *South China Morning Post*, August 27, 2019, <https://www.scmp.com/news/asia/southeast-asia/article/3024479/vietnam-shuns-huawei-it-seeks-build-aseans-first-5g>; and Aftab Ahmed and Sankalp Phartiyal, “India Likely to Block China’s Huawei Over Security Fears -Officials,” Reuters, March 11, 2021, <https://www.reuters.com/world/china/india-likely-block-chinas-huawei-over-security-fears-officials-2021-03-11/>.



1779 Massachusetts Avenue NW | Washington, DC 20036 | P: +1 202 483 7600

CarnegieEndowment.org